GUIDE PRÉPARÉ PAR LE GISF À L'ATTENTION DES ORGANISATIONS NON GOUVERNEMENTALES

gisf

UNOCHA/Antoine Lemonnier

Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS) : Un guide interfonctionnel

Global Interagency Security Forum

À propos de Global Interagency Security Forum (GISF)

Le Global Interagency Security Forum (GISF) est un réseau constitué de nombreuses organisations opérant dans les domaines de l'aide humanitaire, le développement international, les droits humains et la protection de l'environnement, qui estime que la gestion des risques de sécurité (GRS) est un élément important dans ses opérations et la mise en application de son programme. Dans un paysage mondial confronté à des changements rapides, le GISF reconnaît l'importance d'une réévaluation continue de la documentation, de l'adaptation, et de l'innovation des pratiques et politiques de GRS. C'est pourquoi il adopte une approche inclusive de la GRS, et ne croit pas à une sécurité « à taille unique ». Nous reconnaissons que chaque membre du personnel est confronté à des risques différents, en fonction de la diversité de leurs profils personnels, des postes, des contextes et des organisations. En résumé, nous sommes le principal réseau d'ONGs de GRS, et un guichet unique pour le partage d'informations, la gestion des connaissances, la coordination et la collaboration.

À propos des auteurs

Auteure

Beth Chapman (International Location Safety)

Beth est Directrice du niveau des activités opérationnelles et de la gestion de la sûreté et de la sécurité internationale depuis 15 ans. Elle est également Directrice des programmes à International Location Safety (ILS). Elle a travaillé aux côtés de nombreuses ONGs œuvrant dans le domaine de l'humanitaire, du développement, des droits humains et de l'environnement pour l'organisation de visites sûres et efficaces destinées à la planification des programmes dans des environnements complexes, et a procuré le soutien nécessaire aux organisations, pour le développement et la mise en place stratégique et opérationnelle de projets de GRS. Elle est membre du comité BSI SVS/5 et du groupe de travail BS8848:2014. Elle a une parfaite compréhension du devoir de diligence (duty of care), de la gestion des risques de l'entreprise, et de la gestion et de la formation aux risques de sécurité.

Co-auteurs

Nathan Toms (International Location Safety)

Nathan est spécialiste de l'évaluation de la menace, de l'atténuation des risques et du renforcement des capacités des ONGs, des gouvernements, et des forces de sécurité. Il a occupé des postes de haute direction de gestion de la sécurité et la direction des opérations au sein des programmes, dans des contextes politiques complexes comme en Irak, en Ukraine, et au Nigeria. Nathan a été pendant neuf ans officier dans l'armée britannique et a occupé des postes de haute direction dans des ONGs internationales.

Hannah Eastwood (International Location Safety)

Hannah est une Conseillère chevronnée en gestion des risques à International Location Safety (ILS), avec une expérience étendue du conseil en risques stratégiques et opérationnels. Auparavant, elle était Analyste sénior de la menace chez Crisis24 et Palladium au sein du Bureau des affaires étrangères du Commonwealth (FCDO) pour les conflits, la stabilisation, et la médiation. Elle a une vaste expérience du contexte pays, de la Papouasie-Nouvelle-Guinée, de la Moldavie, de l'Ukraine, des EAU, du Rwanda, du Kenya et de l'Indonésie, pour ne citer qu'eux.

À propos de ce guide

Cette ressource a pour vocation de servir de passerelle pour approcher la gestion des risques de sécurité (GRS) à un niveau organisationnel, stratégique et de développement politique. Il ne s'agit pas d'une méthodologie « à taille unique » ou d'un guide pratique. Il s'agit plutôt d'un échange sur les principaux problèmes rencontrés dans la GRS, et de fournir aux cadres supérieurs des pistes de réflexions dans différents domaines, et la façon d'aborder le développement et la mise en œuvre des plans stratégiques de GRS. Cette ressource entend fournir des lignes directrices et participer à l'amélioration de la communication, de la compréhension et de la collaboration entre la GRS, et d'autres dirigeants importants d'une organisation. Ce guide est destiné au personnel directement responsable du développement et de la mise en œuvre de la stratégie et des politiques de GRS au niveau du siège, et à des cadres supérieurs de direction d'autres services stratégiques.

Méthodologie

Ce document a été élaboré en s'appuyant sur 19 entretiens approfondis et semi-structurés avec des informateurs clés (KIIs). Les personnes interrogées étaient des cadres supérieurs responsables de la sécurité au sein d'ONGs humanitaires nationales et internationales, des experts dans leur contexte avec de l'expérience en GRS dans le secteur de l'humanitaire, et des représentants des donateurs et des entreprises. L'accès à cinq ateliers collectifs composés de cadres supérieurs responsables de la sécurité, et deux enquêtes en ligne (avec 23 répondants au niveau stratégique et 29 répondants su niveau opérationnel) ont été mis en place. Un examen approfondi de la littérature a complété ces informations ainsi qu'une analyse finale effectuée par l'équipe de ce guide et de la boîte à outils.

Suggestion de citation

GISF. (2024) Développement de la stratégie et de la politique de gestion des risques de sécurité (GRS) : Un guide interfonctionnel. Global Interagency Security Forum (GISF).

Remerciements

L'équipe ILS a bénéficié des précieux conseils et des contributions des membres du groupe consultatif composé d'experts en GRS, et de praticiens humanitaires de premier plan travaillant dans le secteur. Nous tenons à remercier notamment Owen Dacayan, Neil Elliott, Noemi Munoz, Peter Walsh, Wahidullah Ahmadzai, et Toby Woodbridge pour leurs avis et leurs commentaires d'expert. Le guide a également bénéficié des contributions de spécialistes hors du secteur de la GRS, qui ont partagé leurs connaissances et donné de leur temps en fournissant des contributions importantes, un support et une assurance qualité au projet, méritant ainsi l'immense reconnaissance de nos collègues d'ILS et du GISF. Nous remercions Lisa Reilly (ex- Directrice général du GISF) qui a eu l'idée de la publication de ce document. Nous tenons aussi à remercier Panos Navrozidis, Dimitri Kotsiras, Tara Arthur, Dan Ford et Shaun Bickley, pour leurs révisions et commentaires sur l'avant-projet. Enfin, nous sommes reconnaissants aux équipes du GISF, qui nous ont permis de présenter nos premières conclusions aux Forums d'automne du GISF 2023 à Madrid, et à Washington DC.

IOM/Muse Mohammed

Moldavie
Une travailleureuse humanitaire effectue un sondage auprès d'une réfugiée ukrainienne.

Clause de non-responsabilité

GISF CIC est une société anonyme, immatriculée en Angleterre et au Pays de Galles sous le numéro 14937701. Notre siège social est situé à Romero House, 55 Westminster Bridge Road, Londres, Angleterre, SE1 7JB. GISF CIC est une organisation dirigée par ses salariés. La référence à GISF CIC dans cette clause, inclut les membres du GISF, les observateurs, son secrétariat, et le personnel administratif, les avis ou les opinions exprimés ne représentent pas nécessairement les avis et les opinions des donateurs ou des membres de l'organisation pris individuellement.

Les informations, dans ce document, sont énoncées seulement à titre d'informations générales. Bien que les informations fournies par GISF CIC sont les plus précises et complètes possibles, nous ne garantissons pas la précision, la complétude, expresse ou implicite, de telles informations ni leur fiabilité ou adéquation.

Toute utilisation de telles informations est donc exclusivement à vos risques et périls. Il est nécessaire d'obtenir l'avis d'un professionnel ou d'un spécialiste avant de mener une action ou de s'abstenir de mener une action basée sur le contenu de ces informations. En aucun cas, nous ne sommes responsables, et sans aucune limitation, de la perte ou des préjudices, indirects ou conséquentiels, dus à l'utilisation de telles informations.

Cette publication a été produite par le GISF sous les numéros de subventions 720FDA20GR00341 et 720BHA24GR00016, et financée par l'Agence des États-Unis pour le développement international (USAID) et ChildFund International.

Ce guide doit sa réalisation au soutien généreux des Américains par le biais de l'USAID. Les contenus sont sous la responsabilité du Global Interagency Security Forum et ne reflètent pas nécessairement les opinions de l'USAID ou du Gouvernement des États-Unis d'Amérique.

Table des matières

Acronymes

AI Intelligence artificielle

BoD Conseil d'administration

CINFO Centre suisse de compétences pour les professions de la coopération internationale

CMAG Groupe consultatif civil et militaire

DEI Diversité, égalité et inclusion

DoC Duty of Care (devoir de diligence)

EGC Équipe de gestion de crise

GISF Global Interagency Security Forum

GRS Gestion des risques de sécurité

ISO Organisation internationale de normalisation

KII Entretien avec des informateurs clés

KPI Indicateur clé de performance

MEAL Suivi, évaluation, redevabilité et apprentissage

NSAG Groupe armé non étatique

OCHA Bureau de la coordination des affaires humanitaires des Nations Unies

ONG Organisation non gouvernementale

ONU Organisation des Nations Unies

PSEAH Prévention contre l'exploitation, les abus et le harcèlement sexuel

ROI Retour sur investissement

RSE Responsabilité sociétale des entreprises

SLT Sauvons des vies ensemble (Saving Lives Together)

SOP Procédures opérationnelles standards

ToC Théorie du changement

TRM Gestion des risques de déplacement

Glossaire

Criticité des programmes : cadre utilisé pour la prise de décision sur le risque acceptable, garantissant que l'impact et les besoins des programmes et activités sont équilibrés par rapport aux risques de sécurité.

Continuité des activités : planification stratégique et procédurale qu'une organisation met en place pour garantir que ses fonctions essentielles se poursuivent pendant et après un événement perturbateur.

Duty of care (devoir de diligence) : obligation morale et, dans de nombreux cas, légale, pour un employeur de fournir un niveau raisonnable de protection à son personnel et d'atténuer ou de gérer tous les risques prévisibles susceptibles de nuire à, ou de blesser ses employés, ceux agissant en son nom ou ceux dont il est plus ou moins responsable.

Gestion de crise : planification, coordination et exécution des procédures et des plans d'intervention conçus pour gérer et atténuer efficacement les impacts d'une crise.

Gestion des risques en entreprise/ organisationnels : processus de recensement, d'évaluation, de gestion et de suivi d'un ensemble de risques qui se posent pour une organisation donnée et qui sont susceptibles d'avoir des répercussions sur ses objectifs, opérations, et parties prenantes.

Gestion des risques de sécurité (GRS) : processus et approche de recensement des menaces, d'évaluation des vulnérabilités et des conséquences, et d'atténuation des risques liés à la sécurité des biens, des informations, des personnels et des opérations d'une organisation.

Résilience organisationnelle : capacité d'une organisation à anticiper, à se préparer, à réagir et à s'adapter aux changements progressifs et aux perturbations soudaines.

Introduction

Une stratégie efficace de gestion des risques de sécurité (GRS) est essentielle pour une organisation afin de réaliser sa mission et sa vision. Intégrer et cultiver une culture de GRS forte va au-delà des normes de sauvegarde devant être respectées par le personnel, les consultants, les bénévoles, et du travail avec les organisations partenaires ; c'est un catalyseur pour améliorer l'efficacité opérationnelle, renforcer la conformité aux réglementations et augmenter la confiance des parties prenantes. Par ailleurs, la GRS définit les bases de travail pour des programmes de haute qualité, innovants, et durables à long terme.

Pour atteindre cet objectif, une bonne stratégie d'approche de GRS est nécessaire et requiert à une organisation d'effectuer une analyse approfondie du contexte et des domaines de travail organisationnels afin d'identifier les forces et les faiblesses et de promouvoir une collaboration active entre les équipes et les départements, de renforcer et de mettre en application tous les aspects des programmes et des opérations. Une approche participative, dans laquelle l'organisation évalue continuellement et ajuste ses orientations en réponse aux commentaires internes et aux environnements externes changeants, est également primordiale.

Ce document entend servir de guide stratégique de haut niveau, en positionnant la GRS comme un risque organisationnel, en proposant des orientations complètes sur la manière d'aborder les problèmes interfonctionnels de la GRS, et de les exploiter pour influencer et soutenir des stratégies, des politiques, et des fonctions organisationnelles plus larges. Les responsables de la GRS doivent avoir la capacité d'influencer les membres du Conseil d'administration, les cadres supérieurs et autres fonctions dirigeantes. En procurant des liens vers les débats sectoriels et les bonnes pratiques, ce guide propose des outils pour aider les chefs d'équipes à présenter de manière stratégique les défis que représente la GRS, comment ils peuvent avoir un impact sur l'ensemble de l'organisation, et garantir l'identification et la mise en œuvre de solutions interfonctionnelles efficaces et appropriées.

À qui s'adresse ce guide ?

Ce guide s'adresse au personnel directement responsable du développement et de la mise en œuvre de la stratégie de la GRS au niveau du siège. Il s'adresse aussi aux cadres supérieurs de direction d'autres services stratégiques pour les aider à mieux comprendre pourquoi la GRS doit être présente dans toutes les fonctions et les thèmes abordés.

Comment utiliser ce guide ?

Ce guide a été conçu pour les professionnels de la GRS et les équipes en relation avec la GRS, telles que celles des programmes/ opérations, des RH, de l'informatique, des services financier et juridique. Il procure des outils et des conseils permettant de savoir comment intégrer la GRS dans toutes les fonctions d'une organisation.

Ce guide suit une structure linéaire pour l'élaboration d'une stratégie globale de GRS et la progression vers une politique et mise en œuvre de la GRS, dans les différentes fonctions de l'organisation. Cependant, chaque chapitre souligne un point d'intérêt spécifique permettant aux lecteurs d'aller directement dans la section la plus pertinente pour la stratégie globale de GRS de leur organisation.

- **Chapitre 1** met l'accent sur le processus de développement d'une stratégie de la GRS, et sur les moyens de l'intégrer à la stratégie plus vaste de l'organisation.
- **Chapitre 2** met l'accent sur la place de la GRS dans le cadre de gouvernance de l'organisation et les moyens d'assurer l'engagement des leaders.
- **Chapitre 3** met l'accent sur l'intégration pratique de la stratégie de la GRS dans les différentes politiques et fonctions organisationnelles.
- **Chapitre 4** examine les moyens de renforcer la coordination et la collaboration stratégiques en externe, y compris la collaboration interagences en matière de sécurité.
- **Chapitre 5** met l'accent sur la construction de la résilience organisationnelle par le biais d'une approche agile de la GRS, et l'amélioration de la préparation aux crises.
- Enfin, le **Chapitre 6** aborde l'intégration du système de suivi, d'évaluation, de redevabilité, et d'apprentissage (MEAL) dans le cadre d'une stratégie GRS globale.

1 **Chapitre 1**
Développement de la stratégie de GRS

2 **Chapitre 2**
Gouvernance de la GRS

3 **Chapitre 3**
Intégration interfonctionnelle

4 **Chapitre 4**
Stratégie de GRS Coordination et Collaboration

5 **Chapitre 5**
Contribution de la GRS à la résilience organisationnelle et à la continuité des activités

6 **Chapitre 6**
Suivi, évaluation, redevabilité et apprentissage (MEAL)

En d'autres termes, une stratégie GRS est importante parce qu'elle aligne votre

Chapitre 1 : Stratégie de GRS Développement

organisation sur un seul objectif afin de soutenir votre mission et vision. L'adopter, c'est contribuer à rendre transparentes vos opérations sur le terrain, et faciliter la prise de décision des cadres supérieurs. Autrement dit, une stratégie de GRS doit jouer un rôle clé dans le développement, et permettre de réaliser des stratégies et des politiques organisationnelles plus vastes. L'intégration de la stratégie GRS est cruciale, pas seulement pour obtenir l'allocation d'un budget, mais aussi pour obtenir l'engagement et l'appui de dirigeants stratégiques dans l'ensemble de l'organisation.

1.1 Éléments essentiels de la stratégie GRS

Une stratégie typique de GRS est généralement structurée comme suit :

- Une introduction, dans l'idéal, rédigée par le président-directeur general (PDG), le Directeur Général ou un membre du Conseil d'administration pour défendre votre plan.
- L'objectif ou la déclaration d'intention alignée sur la stratégie organisationnelle en support à la vision générale.
- Vos principes et valeurs (doivent être liés à l'attitude de votre organisation face au risque et à l'approche « duty of care ou devoir de diligence »).
- Un énoncé du contexte (le contexte actuel dans lequel votre cadre de GRS opère, aussi bien en interne (le contexte de l'organisation) qu'en externe (le contexte opérationnel).
- Entre trois et six objectifs stratégiques, thèmes ou buts qui s'alignent avec la stratégie organisationnelle (voir L'outil 1 : Développer ses orientations stratégiques).
- Guide de mise en œuvre et de révision (à court, moyen, et long termes).
- Vous pouvez aussi inclure toutes suppositions dans votre plan, une liste des parties prenantes clés, et détailler les rôles et responsabilités spécifiques (voir le Chapitre 2).

1.2 Intégrer la GRS dans de plus larges stratégies organisationnelles

Les stratégies organisationnelles sont souvent liées à une trajectoire de croissance pour l'organisation, qui peut se traduire par une augmentation de la couverture et de l'expansion des services (donc davantage de personnel), l'ouverture de nouveaux bureaux pays ou par une réponse aux nouvelles situations de crise directement ou avec des partenaires. La sûreté et la sécurité sont essentielles pour assurer la réalisation de ces objectifs. Néanmoins, la GRS n'est pas toujours incluse, en tant que composante interfonctionnelle ou même indépendante, à la planification de ces cycles de programmation pluriannuels

La GRS ne doit pas être vue comme une discussion/ approche séparée ou être introduite pour apporter sûreté et sécurité opérationnelles à une stratégie approuvée. Au contraire, la GRS doit être utilisée comme un facilitateur pour la mission, la vision, et les objectifs stratégiques de l'organisation (voir L'outil 3 : Modèle de planification de la GRS). Une stratégie GRS spécifique doit démontrer comment elle va aider à réaliser les objectifs à long terme de l'organisation, en assurant son devoir de diligence aux personnels, partenaires et associés, tout en offrant une compréhension claire de l'attitude face au risque et des seuils de risque de l'organisation (voir la section 1.5).

Pour intégrer la GRS de manière transparente dans des plans stratégiques plus larges, il est essentiel de lier activement votre stratégie GRS à tous les aspects d'approche globale de l'organisation. Encourager une bonne culture et approche organisationnelles de la GRS implique de faire des efforts pour assurer que les cadres supérieurs comprennent les objectifs de la stratégie GRS et reconnaissent leurs impacts positifs pour l'ensemble de l'organisation.

Pour favoriser cette connexion, votre stratégie GRS doit aussi utiliser le même format, la même langue, et la même structure que la stratégie pluriannuelle de l'organisation. Par exemple, si votre stratégie organisationnelle parle d'orientations ou de thèmes stratégiques, répéter ces mots et phrases dans votre stratégie GRS. Assurez-vous d'énoncer clairement comment la GRS va aider les autres fonctions à réaliser leurs objectifs stratégiques (et vice-versa). Par exemple, si un objectif à long terme de votre stratégie organisationnelle est d'augmenter le nombre de partenaires nationaux engagés dans la programmation, spécifier comment votre stratégie GRS ou ses objectifs spécifiques vont aider l'organisation à atteindre cet objectif. À titre d'exemple, lisez les conseils ci-dessous : « La GRS va développer des procédures de diligence complètes et prioriser les ressources, afin d'offrir un meilleur soutien aux partenaires nationaux ».

En établissant des buts et des objectifs avec des explications claires relatives à la responsabilité et au suivi, et en rendant compte sur ces objectifs, à l'équipe de cadres supérieurs, va également aider à élever et à intégrer la GRS aux discussions de niveau stratégique (voir L'outil 2 : Comment rationaliser votre stratégie GRS).

1.3 Comprendre l'environnement opérationnel et les tendances globales

Toute approche de développement d'une stratégie GRS claire doit commencer par une analyse approfondie du contexte dans lequel le cadre de GRS doit être mis en place en relation avec les priorités du programme. Elle doit prendre en considération le contexte externe (environnemental) et le contexte interne (organisationnel).

L'analyse de l'environnement externe dans tous les domaines doit prendre en compte, par exemple :

- quelles relations l'organisation a avec les parties prenantes externes et mesurer leur importance ? quels besoins ou critères ont ces différentes parties prenantes en ce qui concerne la GRS ?
- quelles lois, règlementations, règles ou normes sont applicables à votre organisation ? comment elles ont un impact sur votre devoir de diligence ?
- quelles sont les tendances externes en ce qui concerne la GRS ? (elles peuvent inclure des changements dus aux attentes du personnel en ce qui concerne la gestion des risques de sécurité, les partenariats et le partage des risques, les nouvelles technologies et les innovations ou les tendances des bonnes pratiques dans le secteur).

L'analyse du contexte organisationnel interne doit prendre en compte :

- les objectifs et les priorités des programmes de l'organisation, la structure et les méthodes opérationnelles ;
- les parties prenantes et comment elles sont impliquées aujourd'hui dans la GRS. Ceci inclut les partenaires de mise en œuvre.
- Quels sont les processus/ procédures de gestion des risques déjà en place ? Est-ce que ces processus et procédures sont actuellement efficaces ?
- Quelle est la structure légale de l'organisation ?
- Quelles sont les polices d'assurance, et de quelles dispositions d'assistance externe l'organisation dispose-t-elle ?

Comprendre la complexité de l'ensemble de votre organisation en répondant à ces questions va vous permettre de développer une stratégie importante et pratique de GRS.

Meilleures astuces : La méthodologie Systemcraft pour le développement d'une stratégie efficace

Systemcraft INSTITUTE

1. Définir votre stratégie en mettant l'accent sur la collaboration.

La GRS ne doit pas être cloisonnée ou envisagée comme une compétence technique que seuls ceux qui la pratiquent peuvent comprendre. La GRS est liée directement à la fourniture du devoir de diligence et assure la continuité des activités, elle est donc importante pour toutes les fonctions d'une organisation. Lorsque la GRS fonctionne bien, une organisation peut rester centrée sur sa mission et atteindre de meilleurs résultats en ce qui concerne les programmes. Dans l'intérêt de tous, il est donc important que la GRS fonctionne de manière efficace. Utiliser ce langage et répéter ces points lorsque vous parlez de la GRS. Faciliter la collaboration en vérifiant quelles sont les structures de partage qui existent déjà et les utiliser. Par exemple, si vous avez déjà un comité de gestion des risques organisationnels, assurez-vous que la sécurité en fait partie.

2. Définir une orientation claire (zoom avant/ zoom arrière).

Toute stratégie nécessite une orientation claire et des interventions à court et à long termes afin de permettre aux personnes de se connecter et de s'engager. À l'image d'un départ pour un long voyage, considérez la recherche d'une stratégie comme une quête vers une destination. Il est toujours utile de prévoir des « arrêts sur le chemin », pour faire une pause, réfléchir, et réévaluer vos objectifs et actions avant de continuer. Définir des objectifs à plus courts termes pour atteindre vos objectifs (de trois à six mois) et à plus longs termes (de deux à trois ans), peut être une approche utile pour la définition de votre stratégie GRS.

3. Faites de la GRS un atout important

Lorsque vous construisez une stratégie, assurez-vous qu'elle englobe ce qui compte pour les autres membres de l'équipe de direction stratégique. Si les personnes doivent faire des changements ou s'adapter, elles ont besoin de comprendre pourquoi c'est important pour elles (et leurs équipes/ départements) Alignez le cycle de développement de votre stratégie GRS avec la mobilisation globale des ressources et du plan stratégique organisationnel. La GRS doit être reconnue comme un facteur clé de succès, tout comme les investissements dans de nouveaux progiciels de finance ou de RH, les flux de travail ou le renforcement des compétences par exemple, qui sont reconnus comme des facteurs clés du succès d'un plan stratégique organisationnel pluriannuel. Engager des discussions avec d'autres départements pour parler de leurs objectifs et problèmes stratégiques. Communiquer dans un langage clair, qui puisse être compris par tous, et orienter la discussion de manière qu'elle reflète les préoccupations et les expériences particulières vécues dans le cadre des propres fonctions.

Meilleures astuces : La méthodologie Systemcraft pour le développement d'une stratégie efficace *(suite)*

4. Changer les motivations.

La plupart des systèmes qui fonctionnent déjà malgré certaines limites, peuvent être à l'origine d'une certaine réticence au changement. Comprendre les raisons pour lesquelles les personnes s'engagent ou ne s'engagent pas dans l'élaboration de stratégies GRS, peut aider à définir et établir de nouvelles motivations. Parfois, cela peut consister simplement à leur fournir l'accès à des technologies ou des applications (par exemple, une application de signalement d'un incident) ou à simplifier le langage ou les procédures afin qu'elles comprennent plus facilement.

5. Tirer parti de l'intelligence collective

Généralement, ce sont les cadres supérieurs qui développent et produisent les stratégies GRS en les mettant à la portée de leurs destinataires (c'est-à-dire, le reste de l'organisation). Un écart peut donc être généré entre les personnes qui définissent la stratégie et les utilisateurs finaux qui doivent la convertir en une réalité opérationnelle. Pour les organisations dont l'intelligence collective est faible, par exemple, un accès limité aux informations et aux analyses provenant du terrain, l'écart est plus grand entre l'approche stratégique et l'approche opérationnelle. Travailler en adoptant une approche participative est donc très important pour la mobilisation de l'intelligence collective à tous les niveaux de l'organisation, en particulier l'intelligence des personnes mettant la stratégie en application sur le terrain.

Dr Simpson, K and Randall, I. (2020), Systemcraft : A Primer

Meilleures astuces : Encourager une approche agile de la GRS

- ✓ Effectuer une analyse SWOT (voir Le modèle d'analyse SWOT sous l'outil 4) – permet d'identifier les forces et les faiblesses de votre organisation ainsi que les opportunités et les menaces que présentent l'environnement opérationnel. Assurez-vous de prendre en considération les éléments politique, économique, social, technologique, légal, et environnemental « PESTLE » hors de votre contrôle, mais pouvant avoir un impact sur vos opérations.
- ✓ Effectuer un exercice de *backcasting*, c'est-à-dire, élaborer une méthode de planification qui commence par la définition d'un avenir souhaitable, puis travaille à rebours pour identifier les politiques et les programmes qui permettront d'atteindre les résultats souhaités. Définir des objectifs SMART spécifique (Specific), mesurable (Measurable), atteignable (Achievable), pertinent (Relevant), et limité dans le temps (Time-bound), et identifier les domaines d'action. Veiller à ce que les canaux de communication sur les progrès et les commentaires soient maintenus.

Meilleures astuces : Encourager une approche agile de la GRS *(suite)*

- ✓ S'assurer que les visions sont alignées, tout le personnel stratégique doit être sur la même longueur d'onde. Faire en sorte que le personnel utilise le même langage, que les indicateurs de signalement soient complémentaires et que les objectifs soient des objectifs communs. Les objectifs de l'équipe doivent être alignés sur les objectifs des fonctions qui doivent tour à tour être alignés sur les objectifs stratégiques de l'organisation.
- ✓ Préparation aux conflits – le travail interfonctionnel rassemble des équipes qui sont habituellement indépendantes, ce qui peut amener les personnes à jouer des coudes pour obtenir de l'influence et des ressources. Il est important de se préparer au conflit. C'est-à-dire, lâcher du lest aux équipes interfonctionnelles afin qu'elles connaissent des échecs et qu'elles puissent ensuite avancer.
- ✓ Intégrer la flexibilité – une stratégie organisationnelle de GRS doit être importante dans tous les environnements opérationnels, mais ce ne doit pas être une approche à « taille unique ». La flexibilité est une clé : Les stratégies de GRS doivent ouvrir des perspectives, et non suffoquer.
- ✓ Augmenter la prise de conscience – la sensibilisation aux processus d'intégration et organiser régulièrement des formations sont des moyens faciles d'intégrer la GRS interfonctionnelle dans la culture de l'organisation.

1.4 Assurer une approche commune de la gestion des risques

En raison de l'interconnexion entre les différents risques, une approche organisationnelle, pour être bien intégrée, doit prendre en considération la gestion des risques dans tous les domaines au lieu de répartir les risques entre les différentes fonctions.

Les organisations ne doivent pas séparer ou prioriser un risque par rapport à un autre, et la GRS doit faire intégralement partie de l'approche de gestion des risques d'une organisation. Lorsque la GRS est considérée comme un élément important de l'approche globale de gestion des risques d'une organisation, il est plus facile de développer une culture de la sécurité holistique et d'inciter les cadres supérieurs à donner leur l'appui et support interfonctionnels.

Développer une approche organisationnelle intégrée des risques doit provenir d'un effort collectif, en mobilisant l'intelligence collective (voir la méthodologie Systemcraft) afin d'évaluer les risques importants autour de la sûreté et de la

sécurité que l'organisation doit affronter, et l'impact potentiel sur la continuité des activités d'une organisation.

La GRS doit figurer au premier plan du processus de prise de décision et constituer un élément clé du cycle de planification de gestion des risques. Regrouper les informations sur les risques de sécurité, les présenter de manière cohérente et les intégrer dans les stratégies globales de gestion des risques de l'organisation est important pour alimenter les politiques et les procédures, et assurer des ressources adéquates afin d'atténuer ces risques dans l'ensemble de l'organisation.

Meilleures astuces : Intégrer la GRS à la gestion des risques de l'organisation :

1. Utiliser un langage simple, non technique.
Éliminer toutes les références techniques et les explications non indispensables lors des discussions et des présentations. Parler plutôt des risques en termes d'objectifs et de résultats favorables pour l'organisation.

2. Lier la GRS à la continuité des activités et à la planification de gestion de crise.
La GRS doit être vue comme un mécanisme de prévention. Elle peut aussi aider à identifier le support nécessaire à la réalisation des objectifs pour l'ensemble des activités, souligner également les éventuels problèmes de sûreté et de sécurité, et travailler avec d'autres départements pour gérer et atténuer de tels risques.

3. Les informations doivent être facilement accessibles.
Commencer par échanger en temps réel les informations sur les menaces externes de sécurité et de sûreté potentielles, et offrir de l'aide aux dirigeants des fonctions pour évaluer- si et comment- elles pourraient affecter leurs domaines de responsabilités. Il s'agit donc de les aider à identifier les déclencheurs spécifiques, de définir des mesures d'atténuation, et d'établir des seuils de risque.

L'analyse et le partage des tendances internes sur la sécurité et la sûreté, sont également importantes pour souligner la valeur d'autres fonctions dans l'organisation. Le partage d'information et en savoir plus sur les incidents et les incidents évités de justesse dans votre organisation, permet aux autres fonctions d'acquérir une compréhension tangible des raisons pour lesquelles les risques de sûreté et de sécurité sont importants pour elles.

4. Développer la prise de conscience à propos de déclencheurs de risque et quantifier les données de risque.
L'intelligence artificielle a permis de créer de nombreuses applications de capture de données, en mesure d'extraire des rapports sur les incidents possibles et les tendances, dans tous les sites et les différents domaines de programmation. L'utilisation de ces outils et des données qu'ils génèrent peut aider les organisations à soutenir et à obtenir des évaluations qualitatives des risques fondées sur

Meilleures astuces : Intégrer la GRS à la gestion des risques de l'organisation : *(suite)*

des interprétations plus subjectives, et à obtenir une plus grande quantité d'informations.

5. Assurer la responsabilisation et la sensibilisation à un niveau plus élevé.
Alors que les responsables des risques sont chargés de la gestion des risques, le conseil d'administration et les cadres supérieurs sont responsables de la surveillance des risques au niveau de l'organisation. Il est important que ces responsables ou au moins l'un d'entre eux soit déterminé, qu'il adopte le bon ton, et qu'il communique clairement l'importance de la GRS à tous les niveaux de l'organisation.

1.5 Définir la stratégie GRS en fonction des risques organisationnels

Une stratégie GRS réussie doit être étayée par l'approche des risques adoptée par l'organisation, il s'agit notamment (a) de l' attitude face au risque, (b) de la tolérance du risque et (c) des seuils de risque. Ces éléments peuvent être très variables en fonction du mandat, de la mission, et des opérations de l'organisation, mais aussi des exigences des donateurs.

Définitions clés

- **Attitude face au risque**, est la quantité de risques qu'une organisation accepte de prendre pour atteindre ses objectifs.
- **Tolérances du risque** sont les niveaux acceptables de variation de l'attitude face au risque de l'organisation, par rapport à des circonstances spécifiques.
- **Seuils de risque** sont les niveaux maximaux d'exposition que l'organisation est prête à accepter.

« La déclaration d'attitude face au risque est généralement la partie la plus difficile à mettre en œuvre dans le cadre de la gestion des risques en entreprise. Cependant, sans seuils de tolérance clairement définis, tout le cycle de risque et tout encadrement du risque est vraisemblablement interrompu ».

L'institut de gestion des risques

La réponse au risque peut être donnée sous différentes formes, par exemple, les formes suivantes identifiées par l'USAID :

- Évitement des risques en ne suivant pas une approche particulière ou en ne signant pas un accord avec un partenaire.
- Réduction des risques grâce à un système fort de contrôles internes, ayant recours à des mesures d'atténuation ou à des formations et des efforts de renforcement des capacités, entre autres options.
- Partage des risques grâce à des partenariats stratégiques avec des parties prenantes clés.
- Acceptation des risques sans atténuation en adoptant les protections appropriées.

Décider de l'équilibre, entre la criticité des programmes (le processus par lequel on détermine des niveaux acceptables de risques pour les programmes d'une organisation) et la GRS peut être complexe, et il n'y a pas d'approche à taille unique (voir la section 1.6 sur le développement d'un cadre de la criticité des programmes).

Les responsables de la stratégie et les cadres supérieurs doivent définir explicitement le niveau de risque que l'organisation est prête ou n'est pas prête à tolérer pour poursuivre sa mission et ses objectifs stratégiques. Il doit être aligné avec sa capacité de risque, c'est-à-dire les niveaux de risque (tolérances) qu'elle peut assumer en relation avec son empreinte opérationnelle, ses ressources, ses capacités et son expertise en gestion des risques.

Il est possible d'effectuer une déclaration d'attitude face au risque (voir L'outil 5 : Exemple de déclaration d'attitude face au risque) qui définit la tolérance au risque de l'organisation et les seuils de risque au-delà desquels l'organisation stoppe ses activités (voir L'outil 6 : Définir une approche organisationnelle des risques).

Meilleures astuces : Différence entre l'attitude face au risque, la tolérance du risque et les seuils de risque

Pensez aux risques associés à la conduite d'un véhicule. Les organisations savent qu'il existe un risque associé à la conduite, et que plus le véhicule roule vite, plus le risque est grand. Cependant, aucune organisation n'insiste sur le fait de ne pas voyager en voiture ou de conduire à 20 km/h, étant donné que l'on ne pourrait pas atteindre la destination souhaitée ou des objectifs stratégiques.

C'est pourquoi, les organisations sont préparées à accepter un certain niveau de risque, mais peuvent mettre en place des mesures raisonnables d'atténuation afin de permettre de gérer ces risques. Par exemple, mettre la ceinture de sécurité ou imposer une limitation de vitesse sont des mesures d'atténuation. Cette approche des risques est souvent qualifiée d'attitude face au risque ou d'appétit pour le risque de l'organisation.

En réalité, il existe toujours une marge de manœuvre qu'une organisation est prête à accepter. C'est-à-dire, la tolérance du risque. C'est dans le même état d'esprit qu'un policier met une amende à un conducteur s'il dépasse moins de 10 pour cent de la limitation de vitesse. Dépasser cette tolérance aboutit éventuellement à un retrait de permis. Il s'agit du seuil de tolérance.

Chapple, M, (2023): Risk appetite vs risk tolerance; how are they different, Tech Target

Établir une déclaration organisationnelle d'attitude face au risque, spécifique pour la GRS peut permettre d'effectuer d'autres évaluations utiles des risques, importantes pour atteindre les objectifs de l'organisation. Sans le cadre fourni par votre attitude face au risque, il est plus difficile pour les équipes de GRS de mener des actions lorsque cela est nécessaire. Par ailleurs, le personnel de l'organisation ne possède pas les informations nécessaires pour prendre les décisions quotidiennes, alignées sur l'approche stratégique de la GRS.

Encourager les employés à prendre des risques éclairés et appropriés fondés sur l'approche organisationnelle des risques (et la tolérance/ possibilité de flexibilité si besoin) peut vous aider à briser la perception d'une GRS « bloquante » qui empêcherait les équipes des programmes d'atteindre leurs buts. L'établissement d'une approche claire et cohérente des risques qui fait l'objet d'une bonne communication, et bien comprise à tous les niveaux peut cultiver de meilleures relations de travail entre la fonction GRS et le reste de l'organisation.

Meilleures astuces : Comment rédiger une déclaration d'attitude face au risque

Définir le contexte : Fournir une brève explication sur la façon dont les risques de GRS sont liés à- ou peuvent avoir un impact sur- l'ensemble de la stratégie de l'organisation en fonction de sa mission, ses buts, ses objectifs, et son contexte opérationnel. Faut-il prendre en considération des facteurs externes ?

Identifier les limites : Spécifier clairement pourquoi il existe une attitude de tolérance zéro, pourquoi il faut adopter une attitude prudente, et pourquoi, dans certaines circonstances, un niveau plus élevé d'acceptation du risque peut être justifié (par exemple, les exigences d'un donateur ou des sites à haut risque inclus dans le programme). Les seuils de risque peuvent être visualisés sur une échelle ou en utilisant la matrice d'Eisenhower qui classe les tâches pour définir leurs priorités : À supprimer, À déléguer, À faire, À planifier

Définir des indicateurs : Définir les indicateurs de risque clés utilisés pour évaluer si l'organisation exerce ses activités dans le cadre de- pas très loin de- ou hors des seuils de risque. Ces indicateurs aident aussi à déterminer un plan d'actions concernant la gestion des différents risques.

Donovan, L (2022), 'What is risk appetite and how do you implement it?', Risk Leadership Network

Comme l'attitude face au risque est souvent une mesure qualitative, les responsables de la stratégie doivent aussi réfléchir au mode de communication de l'attitude stratégique face au risque, à l'ensemble du personnel de l'organisation et aux partenaires de l'organisation. Si la GRS est envisagée comme un processus participatif dans toute l'organisation, qui n'implique pas seulement le personnel de sécurité, cela peut éviter le fossé qu'il existe entre les décisions prises par la haute direction au siège social, et le personnel sur le terrain.

Simples approches pour établir et rendre opérationnelle l'attitude face au risque eu égard à la GRS et au-delà :

- ✓ Affiches donnant une vision claire des seuils de risque clés, tels que la tolérance zéro vis-à-vis du harcèlement sexuel et l'interdiction de conduire pendant la nuit. Ces affiches doivent mentionner les coordonnées des contacts au cas où il serait requis plus d'assistance.
- ✓ Expositions claires des responsabilités – à qui peut s'adresser le personnel pour demander des conseils sur la l'attitude face au risque et les seuils de risque.
- ✓ Alignement sur l'attitude face au risque, un point permanent à l'ordre du jour durant les réunions de planification des programmes.

- ✓ Communications claires lorsque le personnel et les partenaires nécessitent d'être guidés. Il peut s'agir de réunions régulières sur la révision des risques, de conseils sur la réactivité, de canaux de communication dédiés ou d'adresses e-mails pour poser des questions ou demander de l'assistance.
- ✓ Inclusion des politiques, procédures et pratiques GRS dans les nouveaux programmes d'initiation du personnel.
- ✓ Une liste (dans l'idéal pas plus de 10) des règles d'or, facilement traduisibles, qui fournissent des conseils clairs sur les seuils de risque de votre organisation et tout arrêt brutal spécifique. Ces solutions sont adaptables à différents contextes et faciles à comprendre par les partenaires des organisations et le personnel à tous les niveaux.

1.6 Mesurer la criticité des programmes et l'attitude face au risque de GRS

Les impératifs de l'humanitaire et le besoin de toucher des communautés difficiles à atteindre sont des facteurs clés dans le secteur des ONGs. Ils peuvent souvent repousser les limites de l'attitude face au risque d'une organisation. Cependant, la criticité des programmes nécessite un équilibre contre les risques potentiels de sûreté et de sécurité et l'impact qu'ils peuvent avoir sur une organisation en ce qui concerne la continuité des activités. Par exemple, les décès des membres du personnel peuvent affecter la réputation de l'organisation, et se traduire en désastre financier si les donateurs décident de retirer leurs capitaux.

Trouver un équilibre entre la réalisation des objectifs stratégiques de l'ensemble de l'organisation et les risques potentiels de sécurité est crucial. Encadrer la criticité des programmes peut fournir un processus structuré à la prise de décision. Un cadre peut également aider l'organisation à mesurer les risques résiduels contre les principes humanitaires, notamment les principes mentionnant à qui l'organisation vient en aide, et les principes d'humanité et d'impartialité.

Meilleures astuces : Outils pour mesurer la criticité des programmes et l'évaluation des risques de sécurité

Le Cadre de la criticité des programmes est une politique commune du système des Nations Unies pour la prise de décision sur le risque acceptable. Il met en place des principes directeurs et une méthode systématique structurée en vue de mesurer l'utilité des activités impliquant le personnel des Nations Unies à l'aune des risques qu'elles représentent.

UN Programme Criticality Steering Group (2016), United Nations System Programme Criticality Framework, CEB/2016/HLCM/23

Les responsables des risques de sécurité doivent souvent prendre des décisions ou fournir des conseils aux équipes des programmes et aux équipes opérationnelles après que la stratégie de programme a été développée et approuvée. Pour éviter cela, la GRS doit être intégrée aux discussions stratégiques autour de l'attitude face au risque au moment de la planification. Les informations sur les risques et l'analyse des risques de sécurité doivent faire partie de toutes les prises de décision sur les activités et les programmes.

La création d'un comité de gestion des risques interfonctionnel, comptant avec la présence d'un responsable de la gestion des risques de sécurité est un excellent moyen d'y parvenir. Le comité doit s'entretenir régulièrement pour parler des risques, des menaces et des préoccupations émergents, et avoir l'autorité pour prendre des décisions. Par exemple, le comité peut décider de la manière dont une nouvelle zone géographique ou domaine technique au programme est conforme ou dépasse l'approche de l'attitude face au risque de l'organisation dans son ensemble. Voir le Chapitre 2 pour en savoir plus.

Complément d'information

- Systemcraft Toolkit – A Primer
- Strategic Planning for NGOs: A guide to understanding the basics of strategic planning
- How to do Strategic Planning: A Guide for Small and Diaspora NGOs – INTRAC

Syrie

Des chercheurs, en collaboration avec Amnesty International recueille des preuves de frappes aériennes. Obtenir l'accès à des zones dangereuses comme celle-ci peut repousser les limites de l'attitude face au risque d'une organisation.

Chapitre 2 : Gouvernance de la GRS

Une bonne gouvernance et des structures responsables sont fondamentales pour un cadre de GRS efficace. Le personnel, à tous les niveaux de l'organisation, a un degré de responsabilité en ce qui concerne sa sécurité. Cependant, les organisations doivent s'assurer que les structures de gouvernance en place sont efficaces, et que le personnel est conscient et comprend quelles sont ses rôles et responsabilités au sein de cette structure.

La gouvernance de la GRS implique que l'organisation exerce des contrôles réguliers sur les risques auxquels elle doit faire face, et fournisse des orientations pour la sécurité de son organisation. Tout en travaillant dans des environnements complexes et en changement constant, les organisations indépendamment de leur taille, de la complexité de leur mission et de leur empreinte opérationnelle doivent s'assurer qu'elles ont une structure de gouvernance appropriée.

2.1 Intégrer la GRS dans le cadre de gouvernance du risque organisationnel

La GRS peut être intégrée dans l'architecture de la gestion des risques de l'organisation, de manière à promouvoir une culture positive qui contrôle l'ensemble de l'organisation. Elle diffère en fonction de la taille de l'organisation, de l'attitude face au risque et des prestations des programmes. Mais la clé du succès est de s'assurer que son positionnement est correct pour l'organisation.

Les organisations doivent désigner un garant pour le suivi de chaque aspect de la stratégie GRS, et décider comment assurer la gestion de cette approche intégrée dans le cadre global du devoir de diligence afin que rien ne soit négligé ou oublié. Les organisations doivent envisager l'utilisation d'une matrice RACI afin de les aider à décomposer les rôles et responsabilités.

Meilleures astuces : Matrice RACI

L'acronyme RACI signifie :

- **R** – Responsable
- **A** – Approbateur
- **C** – Consulté
- **I** – Informé

Meilleures astuces : Matrice RACI *(suite)*

Responsable

Les responsables sont les exécutants du travail (responsables fonctionnels). Ils doivent mener à bien la tâche ou prendre des décisions. Toutefois, plusieurs collaborateurs peuvent être conjointement responsables.

Approbateur

Cette personne est souvent le chef de projet ou un haut dirigeant. Elle doit signer ou approuver la tâche, l'objectif, ou la décision une fois terminé. Cette personne doit s'assurer que les responsabilités sont assignées dans la matrice pour toutes les tâches. Il n'y a qu'un seul approbateur, ce qui signifie que lui seul peut approuver les tâches et aucun autre.

Consulté

Les consultés sont ceux dont l'avis est recherché avant la finalisation et la signature d'une tâche. Ce groupe de personnes est très impliqué, et sont des participants actifs.

Informé

Ce rôle concerne les individus qui doivent être tenus au courant de l'avancement du projet. Bien qu'ils ne soient pas directement impliqués dans l'exécution des tâches, leur compréhension de l'état du projet est essentielle pour la coordination ou les décisions.

Les personnes responsables peuvent être identifiées en développant les orientations stratégiques de votre organisation (voir la section 1.2).

Un exemple de matrice RACI pour la GRS peut ressembler à cela :

Tâche/ parties prenantes	Tout le personnel	Point focal de la sécurité dans le pays (SFP)	Directeur(e) pays/ régional	Directeur(e) générale de la sécurité	Comité de gestion des risques	Autres fonctions de direction (progammes, RH)	PDG/ Directeur(e) des finances/ Directeur(e) des opérations	Conseil d'administration/ fidéicommissaires
Tâche 1 : Approbation de la politique globale de sûreté et de sécurité	I	C	C	C	R	C	A	I
Tâche 2 : Définition du seuil acceptable de l'attitude face au risque	I	C	C	C	R	C	A	I
Tâche 3 : Développement/ mise en œuvre du cadre GRS (plans pour la sûreté et la sécurité dans le pays, mémos sur la sécurité, plan de gestion des incidents)	C	R	R	R	A	I	I	I
Tâche 4 : Élaboration de la politique de gestion des risques liés aux voyages	I	C	C	R	R	C	A	I
Tâche 5 : Élaboration du plan de gestion de crise pour l'organisation	I	C	C	C	R	R	A	I
Tâche 6 : Renforcement des capacités grâce à la formation en GRS	I	R	R	R	A	I	I	I
Tâche 7 : Passage en revue des incidents, définitions des actions de suivi et partage des leçons apprises	I	R	R	R	A	I	I	I
Tâche 8 : Examen du cadre et de la politique GRS	I	C	C	C	R	C	A	I

RACI

R – Responsable
Les personnes chargées de l'exécution des tâches. Elles sont responsables du travail et prennent les décisions. Plusieurs personnes peuvent être responsables d'une tâche, mais pour que le processus de prise de décision soit plus efficace, essayez de désigner une personne responsable pour chaque tâche.

A – Approbateur
Il s'agit de la personne qui approuve et valide la tâche. L'approbateur n'effectue pas le travail, mais il doit s'assurer que la tâche est accomplie. Pour éviter toute confusion et dilution des responsabilités, il est bien d'avoir un approbateur par tâche au sein d'un projet.

C – Consulté
La personne, la fonction ou le groupe qui aide à accomplir la tâche. La communication avec les consultés est bidirectionnelle, ce qui permet un échange d'informations vital pour la qualité du travail.

I – Informé
Les personnes, les fonctions ou les groupes qui nécessitent d'être tenus informés de l'avancement des tâches. La communication avec les informés n'est pas bidirectionnelle, mais il est essentiel qu'ils soient tenus informés, puisqu'ils sont concernés par le résultat final de la tâche ou du projet.

Adapté par International Location Safety d'après le modèle fourni par Academy to Innovate.

Comprendre la structure de gouvernance de la gestion des risques de l'organisation en suivant cette matrice permet d'assurer que tous les aspects de la GRS sont assignés et incorporés aux autres fonctions également impliquées, et à d'autres compétences (par exemple, les programmes, les ressources humaines, juridiques, et fiduciaires). Ces liens sont détaillés au Chapitre 3.

Tout en assurant une approche interfonctionnelle de la GRS, il est important de réfléchir à une approche inclusive et participative. Pour promouvoir la culture de la GRS, toutes les parties prenantes doivent être impliquées. Leur engagement convertit en réalités opérationnelles les éventuelles conséquences de ces politiques, responsabilise les personnes chargées de la réalisation des objectifs de l'organisation, et promeut une culture positive, durable autour de la GRS.

2.2 Construire une structure sûre et sécurisée efficace

La structure de la fonction de sûreté et de sécurité d'une organisation peut varier en fonction de la taille de l'organisation, du volume et de la complexité de ses programmes, de la maturité de son approche de la gestion des risques, et du nombre de ses effectifs. C'est pourquoi, il est crucial pour les cadres supérieurs d'assurer que la GRS a une position qui permette à l'organisation d'atteindre les objectifs et la mission dans le cadre de ses programmes. La GRS doit donc être intégrée au cadre de gouvernance de gestion des risques, et avoir un rôle déterminant dans les processus de prise de décision.

Toutes les organisations, indépendamment de leur structure, doivent créer un groupe de travail interfonctionnel, un comité ou un groupe pilote, qui représente les différentes fonctions et niveaux de l'organisation. Les membres du comité sont identifiés selon les différentes fonctions, et leurs principales responsabilités définies selon les critères de la matrice RACI dédiée à la GRS. Cette approche collective motive un plus grand sens de la participation, en aidant notamment à la mise en œuvre et à la mise en conformité (voir L'outil 7 : Un exemple des termes de référence (ToR) pour le comité de gestion des risques).

Certaines organisations ont un département tout entier consacré à la sûreté et à la sécurité tandis que d'autres l'incorpore à d'autres fonctions. Quelle que soit la structure, les réflexions importantes pour l'organisation sont :

- La stratégie GRS est-elle dotée des ressources appropriées (humaines et financières) dans la structure actuelle ?
- Avons-nous les connaissances appropriées sur la sûreté et la sécurité dans les fonctions responsables de la GRS ?
- Avons-nous la culture appropriée dans l'organisation permettant de garantir une mise en place efficace de notre stratégie ?
- Avons-nous l'infrastructure immatérielle et matérielle nécessaires pour soutenir la mise en œuvre de la stratégie GRS ? L'infrastructure immatérielle peut inclure le capital humain, des formations complètes, un cadre politique solide, et des accords avec des fournisseurs tiers. L'infrastructure matérielle peut inclure les dispositifs de communication, les équipements individuels de protection, et des bureaux sécurisés.

Si la réponse à ces questions est non, alors l'organisation doit mettre tout en œuvre pour la restructurer ou améliorer les compétences de ses employés afin qu'elle fonctionne efficacement.

Concernant la structure, il n'y a pas de proposition à « taille unique » dans ce document. Mais il contient des réflexions clés, qui doivent être prises en compte, sur les besoins de l'organisation, qui peuvent évoluer avec le temps. Il existe trois structures communes utilisées par les organisations :

- Personnel utilisé pour la sécurité des bâtiments
- Responsabilités intégrées en matière de sécurité
- Fournisseurs externes de sécurité.

Choisir les bonnes personnes dans les bonnes fonctions pour diriger la sécurité est la clé du succès d'une organisation. Exemples, de différentes fonctions :

Personnel utilisé pour la sécurité des bâtiments

Personnes dédiées à la GRS occupant des postes clés dans l'organisation, qui ont des rôles et des responsabilités consacrées uniquement à la GRS. Elles peuvent avoir des responsabilités au niveau mondial, régional et/ou au niveau du pays. Ces fonctions ne doivent pas être nécessairement exercées à tous les niveaux, mais là où il existe un plus grand besoin.

Les pour : Permet aux spécialistes en GRS, dans toute l'organisation, d'élaborer, de mettre en place et d'assurer des cadres de GRS. Fournit des explications claires sur les responsabilités et les redevabilités pour la GRS dans toute l'organisation.

Les contre : Ne garantit pas forcément une culture positive de la sécurité. Les départements de la sécurité peuvent être cloisonnés, cette approche doit nécessairement développer la collaboration entre les départements de GRS et les autres fonctions et un sens collectif de la conscientisation et de la responsabilité. L'élément le plus important étant que la direction reconnaisse le besoin d'une gestion des risques de sécurité active, en tant que partie efficace du programme.

Responsabilités intégrées en matière de sécurité

Certaines organisations n'ont pas de ressources ou préfèrent simplement intégrer les responsabilités en matière de sécurité à d'autres fonctions.

Les pour : Si des cadres de GRS sont en place, et que les personnes donnent de leur temps, leur support, et sont formés, cela fournit une excellente opportunité de responsabiliser les personnes, et de créer une culture positive de la sécurité bien intégrée à la structure de l'organisation.

Les contre : L'intégration des responsabilités en matière de sécurité repose sur le fait que les personnels choisis aient les connaissances et une bonne compréhension de la GRS, et la capacité de mettre en application de telles responsabilités dans toutes leurs tâches. Souvent, les organisations, en essayant d'intégrer les responsabilités de la GRS, échouent, parce qu'elles ne prévoient pas suffisamment de temps, de soutien ou de formation aux personnels.

Fournisseurs externes de sécurité

Certaines organisations passent un contrat avec des conseillers externes en sécurité afin qu'ils agissent en tant que représentants exclusifs de la GRS pour leur organisation ou pour aider d'autres fonctions qui n'ont pas la capacité ou les compétences techniques de gérer la GRS.

Les pour : Les fournisseurs externes de sécurité peuvent apporter leur vaste expérience et des connexions dans des réseaux GRS plus vastes, ainsi que des connaissances des bonnes pratiques dans tout le secteur. Ils ont également un avis extérieur et une opinion impartiale qui peuvent être utiles lorsqu'il faut prendre des décisions difficiles ou comme auditeurs externes avec les recommandations associées à leurs audits.

Les contre : Les fournisseurs externes n'ont pas nécessairement la connaissance intégrée de l'organisation et de ses structures, ni l'approche culturelle de la GRS. Ils peuvent aussi manquer de relations et de connexions internes essentielles pour mettre en place et déployer les cadres de GRS. Notamment, une dépendance excessive aux fournisseurs externes peut diminuer la responsabilité et porter atteinte à la capacité interne et aux connaissances institutionnelles.

2.3 Rôles et responsabilités en matière de GRS

Les rôles et responsabilités autour de la GRS doivent être clairement définis, indiquer clairement qui est responsable de la fourniture de conseils en sécurité, et qui prend les décisions. Utiliser la matrice RACI et comprendre comment, en tant qu'organisation, vous souhaitez structurer la sécurité, vous permet d'établir les rôles et les responsabilités de manière efficace.

Meilleures astuces : Sur les intitulés des fonctions

Si, en tant qu'organisation, vous pensez qu'il est nécessaire d'engager un personnel de sécurité dédié, il convient de réfléchir aux intitulés des postes.

Conseiller en sécurité
Fournit des conseils structurés pour guider les processus de prise de décision d'autrui.

Responsable de la sécurité
Gère la sécurité organisationnelle, y compris la prise de décisions au quotidien.

Meilleures astuces : Sur les intitulés des fonctions *(suite)*

Directeur de la sûreté et de la sécurité/ Bureau du chef de la sécurité/ Vice-président de la GRS
Ces fonctions font partie de l'équipe de direction et ont accès au Conseil d'administration. Ces postes de direction veillent à ce que la sécurité fasse partie du cadre des risques organisationnels, et participent à la sélection d'indicateurs de performance clés (KPIs) trimestriels.

Sauf indication contraire, l'intitulé du poste détermine le niveau d'influence qu'a un individu, notamment sur les activités du programme. Il a déjà été la source de problèmes organisationnelles dus aux conflits entre les départements de sécurité et des programmes. Même si c'est aussi une question de personnalité, l'intitulé d'un poste et l'énoncé clair des rôles et des responsabilités détermine comment l'organisation atteint sa GRS. Il convient aussi de tenir compte de l'étendue géographique de chaque poste. Vous pouvez incorporer des termes comme « national », « régional », ou « mondial » dans les intitulés mentionnés ci-dessus.

Responsabilités organisationnelles

Au-delà de la présentation des rôles et des responsabilités, les politiques doivent également indiquer clairement au personnel les responsabilités de l'organisation, dans la perspective du devoir de diligence, (y compris, au personnel national dans l'éventualité où les cadres et les systèmes juridiques du pays seraient différents).

Les organisations doivent clairement comprendre et communiquer leurs responsabilités vis-à-vis du devoir de diligence moral et légal aux personnels, consultants, bénévoles, et organisations partenaires. Il existe toujours des zones d'ombre, et de ce fait il est préférable que les politiques n'instaurent pas de limites rigides, mais déterminent plutôt qui prend les décisions en fin de compte, et dans quels domaines sont exercées les politiques (voir la section 1.5 sur l'attitude face au risque et la section 3.8 sur la relation avec le domaine légal).

La reconnaissance des cadres supérieurs et l'engagement des dirigeants sont essentiels et la clé du succès. Mais, pour que la GRS puisse prospérer, tout le monde au sein de l'organisation doit accepter un niveau de responsabilité pour sa propre sûreté et sécurité.

Complément d'information

- GISF - Gestion du risque sécurité : Manuel de référence à l'attention des petites ONG
- Mind Tools: How to create a RACI (comment créer une matrice RACI)

Chapitre 3 : Intégration interfonctionnelle de la GRS et du développement politique

Réussir une stratégie GRS repose sur la culture d'un sens commun de la sensibilisation et des responsabilités parmi les cadres supérieurs, et dans l'ensemble des différentes fonctions clés d'une organisation. L'intégration de la GRS est ainsi assurée dans tous les aspects de la planification et des activités de l'organisation.

D'un côté, les cadres supérieurs peuvent jouer un rôle crucial dans la défense de la GRS, et mettre l'accent sur son importance stratégique dans toute l'organisation. D'un autre côté pour assurer l'efficacité de la GRS, il est indispensable que toutes les fonctions dans l'organisation aient conscience de la portée de la GRS dans leurs rôles et responsabilités spécifiques (voir le Chapitre 1). Tout le monde doit également avoir conscience des impacts négatifs potentiels, y compris du coût des incidents, si la GRS n'est pas prise en compte dans le plan stratégique à tous les niveaux de l'organisation.

> *« Les autres départements doivent comprendre les implications de la sécurité dans leurs décisions et activités ».* **(Participant KII, Responsable de la stratégie GRS des ONGs).**

Les organisations peuvent choisir d'approcher les collaborations entre les fonctions stratégiques, de différentes façons. Par exemple, elles peuvent opter pour des groupes de travail, des réunions en face-à-face, les canaux de messagerie en ligne ou des références croisées internes entre les politiques. Peu importe comment, l'essentiel étant de comprendre et d'énoncer clairement comment la GRS se recoupe avec chaque fonction afin d'assurer la résilience organisationnelle à long terme.

3.1 Établir pourquoi la GRS est importante

Dans l'optique que les autres fonctions stratégiques comprennent pourquoi la GRS est importante pour elles, il peut être intéressant de lier la GRS aux quatre piliers de la résilience organisationnelle :

Ces quatre éléments ne sont pas toujours bien compris dans tous les départements. Mais ils doivent être utilisés comme terrain d'entente pour montrer pourquoi la GRS est importante pour toutes les fonctions, et comment elle peut être liée à d'autres risques, tels que :

- Rencontrer les communautés dans le besoin et leur procurer l'assistance nécessaire.
- Augmenter la productivité générale en fournissant un environnement de travail structuré et sûr.
- Fournir l'assurance aux donateurs et aux financeurs que les programmes sont stables, efficaces, et bien gérés, en accroissant donc les possibilités de réinvestissement.
- Protéger les données du personnel, la propriété intellectuelle et les biens.
- Réduire l'exposition légale et financière.
- Permettre aux opérations/ programmation d'accéder aux sites à haut risque.
- Améliorer la réputation et la crédibilité d'une organisation, ce qui peut, à son tour, avoir un effet positif sur la compétitivité, le renouvellement du personnel, et le recrutement de talents.
- Accroître la confiance, le bien-être psychologique et physique du personnel.
- Contribuer à la continuité des activités et à la résilience organisationnelle.
- Démontrer la capacité de l'organisation à contrôler ses risques de sûreté et de sécurité efficacement et intelligemment ce qui peut faire baisser les primes d'assurance.
- Définir des processus plus efficaces pour la gestion de crise.
  (D'après IEC 31010:2019: Risk Management: Risk Assessment Techniques).

La tableau ci-dessous mentionne les domaines spécifiques pour lesquels la stratégie GRS est directement liée à d'autres fonctions afin de favoriser l'exécution des programmes, d'assurer le devoir de diligence, de renforcer la gestion des risques, et d'assurer la continuité des activités. Ces exemples peuvent suggérer des points de départ à des discussions entre les leaders de GRS et les cadres supérieurs d'autres fonctions de l'organisation.

Tableau 1 : Tableau des correspondances entre la GRS et les fonctions organisationnelles clés

Programmes/ opérations	• Accès et prestations de services sécurisés • Planification des programmes • Changement des environnements opérationnels • Changement des environnements de financement • Accès aux partenaires et aux sites de projet • Planification d'urgence (évacuation/ hibernation/ relocalisation) • Sécurisation des environnements numériques, y compris des logiciels et du matériel informatique pour les programmes et les opérations • Support aux partenaires (devoir de diligence, attitude face au risque/ transfert, localisation)
Finance	• Minimiser la perte de biens (personnes/ ressources) • Fraude et corruption (manque d'accès et de surveillance) • Gestion des ressources • Fonds réservé aux situations d'urgence (centralisé ou spécifique à un projet) • Coût des incidents de sûreté et de sécurité (direct et indirect) • Modalités d'assurance
Communications	• Désinformation/ informations erronées • Menaces sur les réseaux sociaux • Communications internes et GRS • Réputation • Représentation publique • Visibilité et image de marque
Informatique	• Cybermenaces • Surveillance numérique • Sécurité des informations et du réseau • Sauvegardes des données
RH	• Diversité, égalité et inclusion (DEI) • Santé mentale et bien-être • Renforcement des compétences • Recrutement et rétention des employés
Juridique	• Définition du devoir de diligence • Devoir de diligence • Travailler avec les organisations partenaires – contrats, juridictions locales, processus réglementaires propres au contexte

Tableau 1 : Tableau des correspondances entre la GRS et les fonctions organisationnelles clés *(suite)*

Sauvegarde	• Sécurité du personnel et des bénéficiaires
Voyages/ Déplacements	• Gestion des risques de déplacement • Analyse du contexte • Autorisation et approbation • Suivi/ surveillance des voyageurs • Évacuation/ relocalisation
Défense* * *abordée au Chapitre 4*	• Coordination civile et militaire • Accès humanitaire • Prestataires de sécurité privée et entreprises militaires privées • Utilisation d'escortes armées • Utilisation de convois

3.2 L'importance d'une GRS agile

Sans des flux de travail interfonctionnels, le partage des informations et des communications, il existe un risque que le département recevant la notification d'un incident ou d'un changement de contexte interprète ces informations sans prendre un autre avis. Il pourrait également oublier de partager ces informations avec d'autres dirigeants chargés de la stratégie et risquer une aggravation du problème ou une augmentation de l'impact de l'incident.

Comme le démontre le Chapitre 1, s'assurer que les cadres supérieurs sachent comment la stratégie GRS est directement liée aux autres fonctions internes, est un excellent moyen de développer une approche agile de la GRS. Tout cela permet à l'ensemble de l'organisation de prendre conscience des éventuelles menaces pesant sur la continuité des activités

3.3 Lien avec les programmes/ opérations

Les équipes chargées des programmes sont principalement impliquées dans l'avancement de la mission organisationnelle. Elles sont souvent sous pression pour atteindre les buts et les objectifs stratégiques clés. La criticité des programmes a donc un rôle important dans la prise en compte des risques de sécurité, et de la GRS, envisagée comme une fonction habilitante et non bloquante. C'est une composante essentielle de l'intégration de la GRS dans les opérations des programmes.

Planification des programmes

Des cloisonnements peuvent se développer lorsque la GRS est perçue comme un obstacle à la réalisation des objectifs des programmes. Ces problèmes peuvent survenir lorsque la GRS n'est pas incluse aux premières phases de développement d'un programme, et considérée comme l'une des dernières exigences avant approbation du programme. Les problèmes peuvent aussi survenir lorsque la GRS est abordée exclusivement comme une fonction de soutien en réponse à un incident.

Les responsables de la GRS doivent travailler en étroite collaboration avec les dirigeants des programmes au moment du développement de leur stratégie respective. En effet, cette façon de procéder va aider le personnel chargé des programmes à reconnaître les avantages de l'intégration de la GRS. Par exemple, les équipes de GRS peuvent travailler avec les équipes chargées des programmes pour identifier quand les activités planifiées/ les sites sont tout près d'atteindre les seuils de risque de l'organisation afin de préparer et d'atténuer ces risques ensemble.

Les responsables de la GRS doivent partager leurs analyses et leur compréhension du contexte mondial, régional, national et des environnements opérationnels, avec les équipes chargées des programmes. En retour, ils doivent utiliser les commentaires et les contributions des personnels chargés des programmes et du personnel local. Tout cela peut aider à contextualiser et localiser les processus de GRS au lieu d'avoir recours à une approche ascendante ou descendante ou à une approche à « taille unique ». Les équipes chargées des programmes sont ainsi soutenues, grâce à des conseils pratiques et réalistes pour atteindre leurs objectifs de manière sûre et sécurisée. Les nouvelles approches et technologies sur la GRS sont également plus facilement intégrées à la planification des programmes.

Les responsables de la GRS et des programmes doivent réussir ensemble à exercer des activités sûres et sécurisées au sein des programmes. Les responsables de la GRS doivent indiquer clairement que l'objectif est de sensibiliser les équipes chargées des programmes à réaliser leurs programmes dans des conditions sûres et sécurisées. La GRS n'est pas bloquante. Avec la GRS, les programmes peuvent être projetés sur le long terme et sont plus durables. Il est également important que ces discussions et décisions soient guidées par l'approche stratégique de l'organisation sur l'attitude face au risque et la tolérance.

Accès humanitaire et exécution des programmes

Les contraintes d'accès peuvent être physiques ou bureaucratiques, le Bureau des Nations Unies pour la coordination des affaires étrangères (OCHA) donne la liste des contraintes les plus courantes pour accéder aux populations affectées :

- Mesures bureaucratiques qui retardent, empêchent ou interfèrent sur les opérations humanitaires.
- Désinformation et informations erronées discréditent les intervenants humanitaires.
- Sanctions et mesures contre le terrorisme qui empêchent le paiement d'honoraires, d'achats ou de matières premières ou l'approvisionnement de marchandises.
- Intensité des hostilités et munitions explosives qui empêchent le déplacement des personnels humanitaires.
- Attaques du personnel et des installations humanitaires, et vol de biens.

L'acceptation est une stratégie clé en matière d'accès et de sécurité. Elle fait référence à la volonté des bénéficiaires, des autorités locales, des belligérants et autres parties prenantes d'accueillir des ONGs humanitaires et de développement dans leurs communautés. Il est primordial que les ONGs cultivent et conservent le consentement des parties prenantes locales pour permettre une acceptation continue. Les ONGs ont ainsi accès aux populations vulnérables et leur permet de s'engager dans les activités des programmes.

Cependant, l'acceptation est de plus en plus sous la menace en raison de l'érosion de l'espace civique dans de multiples contextes. De plus en plus, les gouvernements accusent les ONGs(I) d'affaiblir la sécurité nationale ou d'adopter des valeurs politiques, culturelles ou religieuses qui vont contre les intérêts nationaux. La vie du personnel d'une organisation peut être mise en danger et son accès aux communautés peut être restreint, si une telle organisation donne l'impression qu'elle adhère à un objectif politique ou militaire.

L'opinion d'un expert

« Pour de nombreuses ONGs, l'acceptation est fondamentale pour l'exercice des bonnes pratiques de sécurité. Toute menace à l'acceptation est donc préoccupante pour le personnel de sécurité d'une ONG ».
Morrow, E. (2023) 'Humanitarian Access & Security Management: considerations for staff security'

Les responsables des programmes et de la GRS doivent travailler en étroite collaboration pour développer leur approche stratégique de l'accès humanitaire. C'est particulièrement important dans les situations où les principes humanitaires de neutralité, d'impartialité, et d'indépendance ne sont pas une option ou risquent d'être compromis. Par exemple, il peut s'agir de programmes centrés sur la défense ou le soutien des droits humains. De plus, un lien explicite avec les niveaux politiques et stratégiques entre l'accès humanitaire et la GRS est important pour sauvegarder la durabilité des services dans des communautés difficiles à atteindre.

Meilleures astuces : Élaborer une stratégie efficace de GRS pour la planification des programmes *(suite)*

1. Partager, trianguler et analyser les difficultés d'accès en interne.

Comprendre les types, les causes, et les impacts des obstacles à l'accès est la première étape permettant de les éliminer. Envisager de désigner un groupe de travail au niveau stratégique interne, regroupant les leaders des programmes, de la sécurité, des opérations, et de la communication. Ensemble, ce groupe peut identifier les difficultés, analyser et atténuer les risques, développer des stratégies organisationnelles d'accès, définir des limites à ne pas dépasser (seuils de risque), et des postes dans l'organisation.

2. Former le personnel et créer une culture de partage et des procédures d'escalade

Le personnel de sécurité peut être crucial dans la consolidation des communications, la fourniture de formations, et pour encourager le partage des informations. Il joue un rôle déterminant pour le passage d'une culture organisationnelle de mise en place à tout prix, vers un engagement plus réfléchi et stratégique concernant les problèmes d'accès. Pour les organisations sans personnel d'accès dédié, des procédures d'escalade claires doivent être définies pour que le personnel puisse transférer les problèmes internes et externes à la hiérarchie lorsqu'il ne peut pas les résoudre. Le personnel de sécurité peut soutenir ou diriger l'analyse des risques relative aux problèmes d'accès, et apporter son concours au développement et à la diffusion des politiques internes et des procédures de fonctionnement standards.

3. Prendre les devants dans la construction des relations et le travail de la compréhension.

Construire des relations avec les autorités gouvernementales et les groupes armés non étatiques, le cas échéant, est primordial pour l'acceptation. Même si cela peut être approprié dans certains contextes, ne pas agir au grand jour est rarement une stratégie d'acceptation viable à long terme. La construction des relations et des réseaux est une compétence vitale pour le personnel de sécurité et peut être une ressource précieuse pour guider et impliquer le personnel sur les problèmes d'accès.

4. Mobiliser la communauté humanitaire pour une réponse plus sûre.

Meilleures astuces : Élaborer une stratégie efficace de GRS pour la planification des programmes *(suite)*

Lorsqu'il faut surmonter des obstacles d'accès aux communautés et des problèmes de sécurité, tout le personnel de sécurité des ONGs doit se poser la question : est-ce que ce problème a seulement un impact sur mon organisation ou sur d'autres ONGs et personnes en détresse ? Dans de nombreux cas, la seconde hypothèse est la bonne réponse. En pareilles situations, les problèmes d'accès doivent être partagés et discutés (minutieusement) avec d'autres agences pour trianguler les informations, gérer les risques, et identifier des positions communes avant d'impliquer des partenaires. Tout cela est très important pour encourager l'acceptation des actions humanitaires et favoriser la sécurité du personnel.

Source : Morrow, E (2023) Humanitarian Access and Security Management: considerations for security staff.

Complément d'information

- Frontline Defenders Workbook on Security
- GISF Security Toolbox – Acceptance Analysis (Boîte à outils de sécurité du GISF - Analyse de l'acceptation)
- GISF Achieving Safe Operations Through Acceptance (Le GISF parvient à assurer des opérations sécurisées grâce à l'acceptation)
- Save the Children: The Acceptance Toolkit (la boîte à outils de l'acceptation)

3.4 Lien avec le domaine de la finance

La gestion de la sécurité et de la sûreté génère inévitablement des coûts. Le développement et le déploiement d'une approche complète de la gestion des risques de sécurité peuvent requérir des ressources financières importantes. Les coûts associés à la gestion des risques de sûreté et de sécurité doivent être intégrés aux premiers stades de la planification. Il est important de faire remarquer qu'ils font intégralement partie de la conception du programme et qu'ils sont nécessaires à la durabilité et au succès du plan. De plus, pour un financement efficace de la sécurité, il est important d'appréhender l'importance du potentiel financier associé à un incident de sécurité, et de s'assurer que le risque d'insécurité pesant sur l'entreprise/ les activités est reconnu au niveau stratégique.

Les incidents de sécurité peuvent avoir un impact dans de nombreux domaines d'une organisation.
Par exemple :

- Personnel additionnel interne ou externe pour la gestion de l'incident/ suivi.
- Des relations publiques supplémentaires pour réparer l'image de marque.
- Formation additionnelle.
- Interruptions des opérations liées aux programmes durant l'incident de sécurité.
- Cas de fraude et de corruption ayant pour conséquence une perte financière directe.
- Perte potentielle du financement d'un donateur due à l'incident.

La collaboration entre les responsables des finances et de la GRS est donc essentielle pour le développement d'une organisation mieux préparée et résiliente.

Minimiser la perte de biens/ ressources

Les discussions autour des budgets peuvent être particulièrement ardues pour les professionnels de la sécurité. Dans la plupart des fonctions, il est possible de présenter un retour sur investissement (ROI) prévisible et clair. Cependant, les dépenses de sécurité permettent de prévenir et de minimiser les pertes plutôt que de rapporter de l'argent ce qui est beaucoup plus dur à quantifier pour les décideurs financiers.

Les cadres de GRS doivent présenter la taille de chaque risque et les coûts et pertes potentiels associés, tout comme les autres répercussions, si elles ne sont pas atténuées par les systèmes et les processus de sécurité. Ces remarques peuvent concerner la prévention de la fraude et de la corruption. Les répercussions peuvent correspondre à d'autres risques qui n'ont pas de coûts monétaires directs, mais qui peuvent toujours avoir un effet dramatique sur les résultats financiers. Par exemple, une violation de la sécurité peut nuire à la réputation d'un donateur ou du personnel et avoir pour conséquence une baisse de financement ou de rétention des talents. Ou si une organisation manque de connaissances, le vide créé par le manque de surveillance peut permettre à des activités préjudiciables de prendre racine.

Mobilisation, allocation, et gestion des ressources

La mobilisation, l'allocation, et la gestion des ressources doivent compter avec la sûreté et la sécurité. En règle générale, la sûreté et la sécurité sont les premiers domaines à être touchés par les réductions budgétaires. Elles sont aussi utilisées pour combler les lignes budgétaires d'autres fonctions de support. Les ressources en GRS sont nécessaires pour permettre et soutenir les équipes chargées des programmes dans la réalisation des objectifs stratégiques de l'organisation à long terme.

> *« L'ouverture de nouveaux bureaux locaux ne devrait pas être envisagée à moins que le financement nécessaire aux normes minimales de sécurité opérationnelle soit couvert, tel que stipulé dans les plans de sécurité au niveau du pays ».* - Entretiens KII

Il est important de faire usage des ressources le mieux possible, en éliminant le gaspillage et en produisant un ROI plus élevé. Si elles ne sont pas correctement investies, maintenues et gérées, les ressources en sûreté et en sécurité peuvent épuiser les finances ou occasionner de plus grandes dépenses pour résoudre un problème une fois qu'il s'est produit, plutôt que d'avoir pu le planifier et l'atténuer à l'avance. Par exemple, investir dans la maintenance régulière d'un véhicule et la formation des chauffeurs est plus efficace et économique que d'attendre qu'un véhicule tombe en panne, et prévoir un remorquage d'urgence ou des réparations chères de dernière minute.

Le ROI sur le renforcement de la résilience organisationnelle est aussi un indicateur qui devrait intéresser la plupart des départements financiers. La sensibilisation à la sécurité peut aider à économiser de l'argent en affaiblissant les probabilités d'un incident de sécurité dû à une erreur humaine.

Comment calculer le coût et le financement de la ressource GRS

La ressource du GISF « Le coût de gestion de la sécurité pour les ONGs » explique comment le rapport qualité-prix est souvent l'un des objectifs les plus importants des organisations à but non lucratif. En général, on pense que plus les coûts non liés au programme sont faibles, plus l'organisation est compétente pour allouer la majorité du financement aux dépenses directes du programme. Or, dépenser une grande partie de la donation pour les coûts du programme ne signifie pas forcément que le programme remplit ses objectifs ou les conditions de sûreté et de sécurité (et donc de durabilité).

Une autre pratique commune est d'allouer un pourcentage du budget total du programme aux coûts de gestion des risques. Cependant, les attitudes et les hypothèse sur ce qui est considéré comme pourcentage acceptable varie pour l'ensemble du secteur. Par ailleurs, la gestion du risque de menace, en tant que coût institutionnel générique non lié au programme, est souvent réduit au plus faible niveau possible, pour qu'il soit mieux accepté par les donateurs (en tant que coût indirect), et regardé de manière positive par les organismes externes, comme les auditeurs.

L'alignement avec les cycles budgétaires annuels est important pour l'allocation régulière des ressources nécessaires. Il est également essentiel de travailler avec les équipes financières pour développer la méthodologie régionale nécessaire (qui nécessite son attention). Le perfectionnement des compétences managériales appropriées chez les professionnels de la GRS est aussi une étape fondamentale du processus. Les questions utiles à aborder avec les équipes de la finance sont :

- Votre département accorde-t-il un budget projet par projet ou adopte-t-il une approche plus stratégique ?
- La GRS est-elle soutenue par un financement central ou est-ce qu'elle dépend exclusivement du soutien des donateurs ?
- Prenez-vous en compte le cycle de vie des actifs matériels dans la prévision du budget ?
- Comment pensez-vous financer les plans d'urgence et de préparation ?

Modalités d'assurance

Souvent, les dispositions relatives aux assurances sont décidées par les équipes des finances (ou des opérations), avec pour résultat deux contractions séparées :

- Un manque de communication sur les besoins en assurance de l'organisation concernant les profils de risque des activités des personnels et des sites (c'est-à-dire quels sites, niveaux de couverture et extensions sont nécessaires).
- Un manque de compréhension de la part des locaux sur les démarches à accomplir auprès des assureurs, sur les dispositions spécifiques à mettre en place, et un manque de clarté sur qui est couvert et à quel niveau (par exemple, le personnel international ou le personnel national).

Discuter de ces problèmes, ensemble, avec la direction de la finance, de la GRS et des programmes au moment de la planification stratégique est essentiel pour prendre des décisions sur les assurances compatibles avec les activités du programme, identifier les sites à risque et garantir une couverture d'assurance à tout le personnel.

Complément d'information

- GISF The Cost of Security Risk Management for NGOS (GISF - Le coût de gestion de la sécurité pour les ONGs)
- GISF Securing Aid Worker Security through Effective Budgeting (GISF- Assurer la sécurité des travailleurs humanitaires grâce à une budgétisation efficace), (page 76)

3.5 Lien avec le domaine des communications

Les équipes de communication et de GRS doivent se soutenir mutuellement aussi bien en interne qu'en externe. D'un point de vue externe, les fonctions de communication et de GRS doivent travailler en collaboration pour gérer et atténuer les risques que présentent les informations erronées ou la désinformation, les réseaux sociaux, et les incidents de sécurité. En interne, les responsables de la communication peuvent jouer un grand rôle dans le maintien et l'amélioration de l'efficacité du cadre de GRS, en soutenant les responsables de la GRS, pour simplifier les messages et sensibiliser le personnel.

Définitions clés

- **Informations erronées :** informations fallacieuses, mais dont la source n'a pas l'intention de nuire.
- **Désinformation** : fausses informations dont la source diffuse volontairement de fausses informations à l'opinion publique.

Désinformation et informations erronées

La désinformation et les informations erronées augmentent rapidement les risques pour les organisations, en particulier pour celles qui interviennent dans des environnements politiques à haut risque. L'impact sur la sécurité peut être considérable. Par exemple, de fausses déclarations peuvent faire arrêter le personnel des ONGs ou qu'il subisse une attaque physique.

Il est important de comprendre que les menaces de sécurité en ligne peuvent directement nuire à la sécurité physique du personnel ou aux personnes en relation avec l'organisation. La diffusion d'informations erronées ou la désinformation en ligne peuvent aboutir à une colère générale qui peut être utilisée pour justifier des attaques physiques.

La désinformation ou de fausses informations peuvent aussi semer la confusion pour distinguer les vraies des fausses informations. Les professionnels de la GRS ne peuvent donc pas se fier aux médias pour les aider à recueillir des informations sur un lieu, et prendre des décisions délicates, notamment en période de crise ou d'urgence. Dans ces situations, les experts en sécurité sont forcés de faire le tri entre les vraies et fausses informations ce qui peut prendre un temps précieux. La possibilité, pour ces organisations et individus, d'offrir une aide rapide pour sauver des vies, et dans le pire des cas celles de leur personnel, est donc entravée. La nature des communications numériques et les menaces qu'elles représentent exigent des solutions interdisciplinaires. En réaction, les organisations doivent mettre en relation les différents départements de communication qui font généralement appel à des spécialistes des réseaux sociaux et des technologies des communications en ligne, avec les équipes de GRS de manière qu'ils puissent échanger des idées sur la meilleure stratégie de gestion et d'atténuation des risques concernant la diffusion de la désinformation.

Les responsables des communications peuvent soutenir les responsables de la GRS pour développer des modalités dynamiques d'identification et de réponse à la désinformation, et passer de systèmes de réponse *ad hoc* à des flux de travaux plus simples sur la gestion de la désinformation.

Réseaux sociaux

Les réseaux sociaux sont une partie primordiale des communications, de la défense, et des stratégies de marketing de l'organisation. Mais les menaces associées aux réseaux sociaux sont en pleine expansion et présentent des risques directs, cruciaux, pour la sûreté et la sécurité du personnel et la réputation de l'organisation. Il est recommandé d'envisager une approche large au niveau de l'organisation pour le développement des stratégies des réseaux sociaux, et d'impliquer le personnel de gestion des risques de sécurité.

Par exemple, les équipes de communication pourraient ne pas être au courant de certains messages publiés sur les réseaux sociaux pouvant affecter la sûreté et la sécurité du personnel dans un contexte particulier. Pareillement, le personnel, les consultants et les bénévoles doivent aussi être tenus informés des questions de sûreté et de sécurité sur l'utilisation des réseaux sociaux afin de pourvoir partager les mises à jour concernant le travail sur leurs profils personnels.

Communications internes

Développer de bonnes communications internes autour de la GRS est primordial pour assurer l'engagement, et un déploiement correct de toute stratégie de GRS (voir le Chapitre 1). Travailler avec les responsables de la communication pour simplifier les messages internes de GRS, et la traduction des messages clés de GRS dans différents contextes, peut constituer un actif énorme.

Les modes de communication peuvent inclure du contenu de la plateforme sociale interne, tel qu'une page Intranet ou la lettre d'information. Vidéos, réunions-débats, événements en ligne en face-à-face, e-mails et diffusions en direct du personnel clé, sont d'autres options viables de communication sur la GRS.

Communications externes

Traiter un incident de sécurité requiert aux équipes de travailler avec plusieurs départements et dans plusieurs domaines. Les personnes traitant les incidents de GRS sont tenues de gérer et atténuer l'impact de l'incident, tandis que les équipes de communication mettent au point une réponse publique. La manière dont une ONG répond ou ignore la divulgation au public d'un incident de sécurité affecte grandement sa réputation et sa capacité à continuer de fonctionner de manière sûre.

Une communication, préparation et planification claires entre ces deux fonctions sont donc essentielles.

Les responsables des communications et de la GRS peuvent et doivent également travailler ensemble au développement d'approches stratégiques dans le cadre de la représentation publique autour de la GRS. Par exemple, travailler avec les responsables des communications pour le développement de messages externes, autour d'un bon devoir de diligence, et comment ce facteur renforce la résilience organisationnelle

Complément d'information

- InterAction Risk Assessment Tool: Assessing organisational risk related to disinformation (p.25).
- Internews: Managing Misinformation in a Humanitarian Context
- CDAC Network
- GISF's Security Risk Management Toolkit: Strategies (Boîte à outils de gestion des risques de sécurité du GISF : Stratégies) (pages 14 et 15)

3.6 Lien avec l'informatique

Aujourd'hui, de nombreuses fonctions de sûreté et de sécurité intègrent la sécurité numérique pour une approche de plus en plus holistique de la GRS. La manière dont le personnel peut se protéger et réduire son exposition individuelle aux menaces en ligne est incluse dans cette approche. Cependant, cela peut créer parfois une déconnexion entre la gestion du risque de sécurité numérique, l'étendue et les responsabilités des départements d'informatique (qui sont davantage orientés sur les menaces de cybersécurité au niveau de l'organisation).

Les responsables de l'informatique et de la GRS doivent partager leurs approches des cybermenaces et des menaces numériques et communiquer leurs mesures d'atténuation pour la gestion des risques en ligne. En effet, ces démarches ont un impact direct sur l'amélioration de la sûreté et de la sécurité du personnel et sur la continuité des activités.

Définitions clés :

- **Cybersécurité :** protège les réseaux, les comptes, les systèmes informatiques ainsi que les informations sur l'utilisateur.
- **Sécurité numérique :** protège votre présence en ligne, les données à caractère personnel, les biens et les informations.
- **Sécurité des informations :** protège la confidentialité, l'intégrité, et la disponibilité des informations.

Convergence de la sécurité physique, numérique, et la cybersécurité

Les menaces en ligne peuvent avoir un lien direct avec la sécurité physique. Par exemple, la surveillance numérique peut démasquer des acteurs malfaisants qui accèdent ou partagent les informations personnelles en ligne d'une personne avec d'autres cybercriminels. Ces pratiques pouvant permettre au voleur de données ou à une autre personne malfaisante qui y a accès, de harceler ou de nuire physiquement aux individus.

Tout comme pour les menaces de sécurité numérique individuelles, les cyberattaques au niveau de l'organisation peuvent également avoir un impact sur la sûreté et la sécurité physique des individus. En raison de la nature confidentielle des données humanitaires et du caractère politique du travail humanitaire, la perte des données à caractère personnel dans le cadre d'une cyberattaque à grande échelle peut être catastrophique. Elle peut affecter non seulement les employés, mais aussi les personnes que l'organisation cherche à aider, en augmentant le risque d'une attaque physique ciblée.

Exemple dans ce secteur : Cyberattaque majeure contre le Comité International de la Croix Rouge (CICR)

En janvier 2022, le CICR a dû faire face à une violation de la cybersécurité majeure, exposant les données à caractère personnel de plus de 515 000 personnes dans le monde. La violation qui a inclus des données à caractère personnel tels que les noms, les lieux, et les informations de contact, a affecté des personnes disparues et leurs familles, des détenus, et autres personnes, recevant des services de la Croix Rouge Internationale et du Croissant rouge, à cause d'un conflit armé, de désastres naturels ou de crises migratoires.

Cette violation des données a mis en évidence une tendance préoccupante des cyberopérations ciblant les organisations humanitaires. Ces genres d'attaques font encourir de graves risques aux populations déjà vulnérables pouvant subir des préjudices dus à l'exposition de leurs informations sensibles.

En réaction à la violation, le CICR travaille désormais en collaboration avec ses partenaires du Croissant Rouge pour renforcer le cadre légal et politique pour la protection des données et de l'infrastructure des organisations humanitaires. Ils sont très actifs auprès des gouvernements pour améliorer les protections en ligne.

Lire la suite : https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Même lorsque les organisations ou les individus ne sont pas directement ciblés, ils peuvent encore être impactés comme lorsqu'une cyberattaque est commise contre un intervenant privé avec qui l'organisation ou une personne a une relation. En 2020, SolarWinds, une société d'informatique américaine, a été piratée, et une bonne partie de ses données ont été volées. Comme la société hébergeait les données de nombreuses autres sociétés, les agences gouvernementales, les organisations à but lucratif, et bon nombre de différentes organisations se sont fait voler leurs données et leurs informations.

Ce piratage a mis en danger la santé et la sûreté de ceux dont les données étaient hébergées par SolarWinds.

L'opinion d'un expert

« Les cyberattaques mettent une grande pression sur les ressources limitées des ONGs, les empêchent de remplir leurs missions à court terme, mais peuvent aussi nuire à leur réputation à long terme, compromettre la confiance en leurs capacités à assumer leurs rôles durant les situations de crise et d'urgence actuelles et futures ».
Reliefweb, 'Cyberattacks; a real threat to NGOs and not-for-profits', 2022

Il est crucial d'améliorer la communication et la coordination entre les responsables informatiques qui travaillent directement à la gestion des cybermenaces organisationnelles, et les personnes qui développent des stratégies de GRS afin de protéger le personnel des menaces sur la sécurité numérique. Les lacunes et les faiblesses du profil de cyberrisque d'une organisation sont souvent dues à un manque de compréhension des risques au niveau humain. Les équipes de GRS et d'informatique doivent travailler en étroite collaboration pour identifier les menaces clés, évaluer où se situent les lacunes potentielles, et développer les approches de formation et de support pour le personnel à tous les niveaux de l'organisation.

Simplifier le langage technique

Évaluer et présenter les risques de cybersécurité et de sécurité numérique dans un langage non technique est également important pour impliquer les responsables de gestion des risques organisationnels, et permettre que les décisions prises au niveau stratégique tiennent compte des risques. Présenter les risques et les mesures d'atténuation dans un langage simple qui décrit l'impact qu'ils peuvent avoir sur les opérations de l'organisation est essentiel. Enfin, une telle présentation peut garantir que ces risques sont pris suffisamment au sérieux, et aider les organisations à opérer les changements nécessaires pour devenir plus sûre.

Complément d'information

- GISF Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks (Les travailleurs humanitaires du GISF à une époque d'incertitude : le recoupement des risques numériques et physiques)
- Integrating Cybersecurity and Enterprise Risk Management (ERM)
- GISF Security to Go: Module 4 Digital Security (GISF - Prise en main rapide de la sécurité - Module 4 : La sécurité numérique)
- GISF Digital Security of LGBTQ+ Aid Workers (La sécurité numérique des travailleurs humanitaires LGBTQ+ du GISF)

3.7 Lien avec les ressources humaines

La relation entre les RH et la GRS est essentielle à la planification, la gestion et l'atténuation efficace des risques de sûreté et de sécurité pouvant affecter le personnel dans tous les environnements opérationnels. Même si les domaines de responsabilités sont clairement différents entre les fonctions de RH et de GRS, il existe une forte interdépendance, qui est fondamentale pour remplir le devoir de diligence d'une organisation.

L'article du GISF « Vers une gestion inclusive des risques de sécurité » indique que les ONGs tiennent de plus en plus compte des profils du personnel humanitaire qu'elles engagent et déploient, pour maximiser l'acceptation et atténuer les risques. Établir des systèmes qui reconnaissent et acceptent différents profils de personnel, permet de mieux comprendre les risques auxquels chacun est confronté et s'assurer que des mesures adéquates sont en place pour les atténuer est vital pour améliorer l'accès et maintenir le personnel en sécurité. Cependant, la stratégie d'atténuation des risques ne peut pas se contenter simplement d'identifier des profils de collaborateurs. Les responsables des RH et de la GRS doivent aussi collaborer pour s'assurer que ces approches adaptées de la sécurité et ces mesures spécifiques sont communiquées de manière adéquate à chaque membre du personnel. Les ressources partagées ci-dessous proposent d'autres exemples sur la manière dont les organisations peuvent améliorer leur approche centrée la personne.

Diversité, égalité, et inclusion (DEI)

Comme la sécurité, la DEI est interfonctionnelle, elle a des fonctions bien précises ou des points focaux dans toute l'organisation. Bien que la DEI soit structurée ou citée, dans une organisation il existe toujours un lien intrinsèque avec les RH et la GRS. Pour favoriser un environnement opérationnel plus sûr et inclusif, les RH et la GRS doivent développer ensemble un cadre pour le partage des informations essentielles de sûreté et de sécurité. Impliquer les professionnels et les pratiques de la DEI, peut garantir que les informations de sécurité sont diffusées aux différentes catégories de personnels. C'est à dire à tous les personnels, indépendamment de l'ethnie, la race, la religion, des handicaps mentaux ou physiques, de l'identité sexuelle, et bien plus encore. Certains facteurs incluent également les besoins médicaux et l'expérience antérieure.

Meilleures astuces : Terminologie et acronymes pour la DEI

La DEI a plusieurs appellations en fonction de l'organisation et des objectifs de cette fonction. Voici quelques exemples parmi d'autres, GEDI (Genre, Égalité, Diversité, Inclusion), JEDI (Justice, Égalité, Diversité, Inclusion). Il existe des cas pour lesquels cette fonction peut être indépendante des RH, bien qu'il subsiste toujours des interdépendances.

Fournir des possibilités sûres et sécurisées qui encouragent le personnel à signaler les préoccupations, les incidents, et les incidents évités de justesse, en particulier lorsqu'il s'agit de profils spécifiques peut également aider les organisations à réfléchir, à revoir leurs pratiques, et à procéder à des modifications si nécessaire. Les mécanismes pour y parvenir n'ont pas besoin d'être complexes, et peuvent améliorer les bonnes pratiques de GRS. Certains exemples montrent qu'il y a une représentation transversale du personnel, pendant le développement des évaluations des risques ou la redynamisation des processus, afin de recueillir les commentaires en cours. En travaillant avec les professionnels de la DEI et des RH, la GRS peut rester agile et répondre aux besoins intersectoriels du personnel.

Santé mentale et bien-être

La GRS va au-delà de la sécurité physique pour inclure la sécurité psychologique. Le personnel devrait avoir accès à des espaces sûrs pour préserver sa santé mentale ou recevoir le support nécessaire pour les créer. Ceci pouvant avoir un impact extrêmement positif sur les activités du programme et les objectifs stratégiques à long terme.

Les dangers et les angoisses inhérents au travail humanitaire, font qu'il est particulièrement important que les organisations humanitaires prennent des mesures pour la protection de la santé mentale de leurs employés. Le podcast du GISF sur la sécurité psychologique parle des problèmes de santé mentale et du bien-être dans le secteur humanitaire. Les problèmes de santé mentale peuvent souvent avoir un impact sur la santé physique. De même, les maladies mentales non traitées et les problèmes de santé physique qui en découlent peuvent s'accumuler et entraîner des dépenses importantes pour la personne et son employeur. Par conséquent, faire de la santé mentale une sous-priorité comporte un risque important pour les entreprises.

De récentes recherches menées par McKinsey & Company prouvent qu'une forte sécurité psychologique est l'un des plus puissants indicateurs de la performance, la productivité, la qualité, la sécurité, la créativité, et l'innovation d'une équipe. C'est également l'indicateur d'une meilleure santé, globalement. Améliorer les conditions dans lesquelles les organisations créent et maintiennent des environnements psychologiquement sûrs peut avoir des impacts positifs mondiaux sur la sécurité d'une organisation. La sécurité psychologique permet aussi de promouvoir une culture de la sécurité inclusive et d'obtenir des résultats transversaux.

Une relation constante et forte entre les responsables de la GRS et les RH est indispensable pour atteindre cet objectif. Cette relation est particulièrement importante dans les domaines de la rétention du personnel, du signalement des incidents, et des efforts stratégiques continuels pour renforcer la culture de l'organisation autour de la santé mentale et du bien-être.

De nombreux progrès ont été faits auprès des directions pour les sensibiliser aux besoins en santé mentale des personnels travaillant dans le secteur de l'aide. Il reste cependant encore beaucoup à faire au niveau stratégique pour sensibiliser les dirigeants et discuter de la mesure dans laquelle une mauvaise santé mentale des personnels peut avoir des répercussions sur les objectifs organisationnels. Les discussions entre les responsables de la stratégie des RH et de la GRS sur les moyens d'atténuer ces risques sont fondamentales. Elles sont particulièrement importantes dans les domaines les moins documentés. Par exemple, pour les cas de traumatisme indirect, et pour le personnel de soutien provenant de différents contextes culturels ou opérant dans des contextes où, par exemple, la santé mentale et le bien-être ne sont pas aussi largement reconnus ou abordés.

Recrutement et rétention des employés

De nombreuses organisations trouvent qu'il est de plus en plus difficile d'attirer, de former, de retenir et de motiver du personnel compétent en GRS. Il s'agit d'une inquiétude majeure qui peut avoir de graves impacts sur les opérations et la résilience d'une organisation. En raison du paysage toujours changeant, les restrictions financières viennent s'ajouter aux vulnérabilités touchant déjà le recrutement et la rétention du personnel. Ajoutées aux difficultés de certains professionnels de la GRS à démontrer leur rôle déterminant à l'aide d'indicateurs de performance clés qui ne sont pas toujours en phase avec les objectifs stratégiques, il est encore plus difficile d'informer et d'influencer les décideurs au niveau stratégique. Par exemple, un professionnel qualifié de GRS n'a pas nécessairement accès ou n'est pas forcément rattaché aux décideurs clés de l'organisation ou aux cadres exécutifs. Pourtant, ils sont toujours mandatés pour encourager une meilleure culture de la sécurité.

Les responsables des RH et de la GRS doivent aussi discuter et revoir régulièrement leur approche du recrutement et de rétention du personnel de GRS. Plutôt que d'utiliser le même ensemble de spécifications et de compétences pour l'ensemble du personnel GRS, une approche stratégique plus adaptable doit proposer une plus grande flexibilité en ce qui concerne l'expérience et les compétences requises pour les fonctions spécifiques de l'organisation.

Renforcement des compétences

Identifier les besoins en apprentissage et en développement est une partie clé de la planification au niveau stratégique, en comptant sur la collaboration des responsables de la GRS et des RH (voir L'outil 8 : Modèle de plan de développement et d'apprentissage). Définir des objectifs stratégiques visant à renforcer la capacité du personnel de la GRS doit être envisagé comme un investissement plutôt que comme une dépense supplémentaire (voir L'outil 9 : Exemple de matrice pour la formation stratégique). Dans cette optique, il est important d'assurer une approche stratégique pour la formation professionnelle continue, qui présente et encourage les opportunités de progression et d'avancement du personnel de la GRS, lui permettant de rester souple face aux besoins de changement, tout en approfondissant les bonnes pratiques.

Complément d'information

- GISF Managing the Security of Aid Workers with Diverse Profiles (Gérer la sécurité des travailleurs humanitaires avec différents profils du GISF)
- GISF Towards Inclusive Security Risk Management (GISF -Vers une gestion inclusive des risques de sécurité)
- GISF Security to Go: People Management (GISF- Prise en main rapide de la sécurité : la gestion des personnes)
- GISF Podcast – psychological safety episode (Podcast du GISF - épisode sur la sécurité psychologique)
- McKinsey & Company: What Is Psychological Safety?
- GISF Humanitarian Security in an Age of Uncertainty: The Intersection of Digital and Physical Risks (Les travailleurs humanitaires du GISF à une époque d'incertitude : le recoupement des risques numériques et physiques)

3.8 Lien avec le domaine légal

Les fonctions du domaine légal et de la GRS partagent un objectif commun : protéger une organisation des dangers. Grâce à une collaboration et communication étroites, chaque fonction peut aider autrui à optimiser la sécurité et la conformité dans l'ensemble de l'organisation. Il est également inévitable que les différentes lois affectent le travail de l'équipe de sécurité. Déterminer quels cadres de travail réglementaires sont applicables n'est que la première étape, étant donné que les responsables juridiques et de GRS doivent discuter et décider de l'interprétation des réglementations dans des contextes opérationnels spécifiques.

Satisfaire les exigences du devoir de diligence

Le devoir de diligence fait référence à une exigence juridique (et morale) de l'organisation à suivre toutes les étapes nécessaires pour assurer le bien-être physique et mental de son personnel. Bien que toutes les organisations aient une bonne compréhension des modalités d'application du devoir de diligence à leurs employés directs, des complications surviennent au moment d'établir les responsabilités entre :

- Le personnel exerçant dans différents contextes légaux.
- Le personnel travaillant sur différents types de contrats, comme le personnel international, le personnel national, les consultants, les bénévoles et les personnes à leur charge.
- Le personnel travaillant pour des partenaires extérieurs ou des consultants extérieurs.
- Partenaires de mise en œuvre (voir Source d'information du GISF: Gestion de la sécurité et développement des comptétences : Agences internationales travaillant avec les partenaires locaux).

Meilleures astuces : Outil d'auto-évaluation du devoir de diligence

Le Swiss Centre of Competence for International Cooperation (CINFO) et le GISF ont développé un outil complet d'auto-évaluation du devoir de diligence Il permet aux organisations d'évaluer les questions de sûreté et de sécurité en matière de devoir de diligence. Les outils proposent cinq étapes, de l'étape initiale à un niveau optimisé pour la détermination des points forts d'une organisation, et des domaines d'amélioration dans quatre domaines : information, surveillance, prévention, et intervention.

Source d'information : https://dutyofcare.cinfo.ch/index.html

Exemple dans ce secteur :

« Le partage des risques était un défi majeur pour nous lorsque nous travaillions avec des consultants et des partenaires de l'organisation. Nos clients et partenaires de mise en œuvre ont souvent eu du mal à envisager un certain degré d'obligation de diligence pour un consultant qui n'était pas leur employé ou sous-traitant. Pour éliminer ce problème nos équipes de sécurité et juridique ont rédigé de nombreux protocoles d'accord pour clarifier les fonctions, car personne n'était clair sur qui devait assumer telle ou telle responsabilité. Les projets étaient donc parfois considérablement retardés, et les processus devenaient trop lourds en termes de ressources ».

(Participant KII, SFP des ONGs au niveau opérationnel)

« La question du devoir de diligence en termes médicaux, pour le personnel national de ma dernière organisation, signifiait que lorsqu'un membre du personnel avait un accident de voiture et qu'un chirurgien n'était pas disponible pour empêcher l'amputation, nous devions le transporter en avion de Somalie en Éthiopie et financer les coûts additionnels des soins et de physiothérapie ».

(Participant KII, Responsable stratégique des ONGs)

Du point de vue stratégique, il est essentiel pour de nombreux responsables de savoir où se situent les complications concernant le devoir de diligence, et de déterminer où se situent les responsabilités. Les équipes de GRS, des RH, et juridiques sont amenées à effectuer des représentations graphiques des parties prenantes afin de pouvoir formuler et évaluer clairement les complications concernant le devoir de diligence de leur organisation. Les résultats de ces activités peuvent être ensuite utilisés dans la planification stratégique et la mise en œuvre pratique.

Exemple de représentation graphique des parties prenantes :

Partie prenante	Devoir de diligence direct	Devoir de diligence partagé	Devoir de diligence moral
Employé direct à temps plein, à temps partiel	X		
Consultant (interne)	X		
Bénévole	X		
Visiteur	X		
Personnel de partenaire de mise en œuvre		X	
Consultant (organisation externe)		X	
Personnel détaché auprès d'une organisation externe		X	
Employé d'une association membre			X
Bénéficiaire			X
Personne à charge d'un employé			X
Lorsque le devoir de diligence est partagé, il doit être réparti entre les organisations partenaires. Des accords clairs ou des protocoles d'accord doivent être mis en place, en définissant les responsabilités, les attentes, et des normes minimales concernant le devoir de diligence.			
S'il s'agit d'un devoir de diligence moral, une organisation doit clairement présenter le support, les ressources, et les mécanismes utiles. Orientations et conseils doivent aussi être fournis, mais la partie prenante n'a aucune obligation légale.			

Créer une culture de compréhension atour du « devoir envers les individus »

Les employeurs ont un devoir de diligence envers leur personnel. Toutefois, les employés ont également le devoir vis-à-vis de leur organisation de participer activement à la planification de la sûreté et de la sécurité, de suivre les procédures de fonctionnement standards et d'urgence selon les politiques de la société, et de faire preuve de bon sens afin d'éviter les risques inutiles durant les activités qu'ils effectuent au nom de leurs employeurs.

Dans l'idéal, les tâches organisationnelles et individuelles marchent main dans la main. Ensemble, elles créent une culture où les employeurs prennent soin de la santé, de la sécurité, et du bien-être de leurs employés. Les employeurs doivent développer et déployer des politiques, des procédures, et des conseils appropriés en GRS, afin de protéger le personnel des dangers.

À leur tour, les employés doivent s'engager activement et suivre ces protocoles.

Pour créer cette culture de responsabilité conjointe au niveau stratégique, il est nécessaire de créer une relation sûre et réciproque entre l'employeur et l'employé. Les employés doivent agir de manière sûre et responsable, mais les employeurs doivent aussi être proactifs quant à la définition de paramètres appropriés. Fixer des objectifs non réalistes au niveau stratégique a pour conséquence un manque d'engagement si le personnel sent qu'il ne peut pas atteindre concrètement ses objectifs en travaillant avec ces partenaires.

Il est donc essentiel de définir la position organisationnelle sur le devoir de diligence et les attentes des individus. Elle ne doit pas être seulement basée sur les obligations contractuelles, mais aussi sur les commentaires et la participation du personnel. Mettre au point des moyens clairs et faciles de faire des commentaires est un point de départ judicieux.

Quelques options :

- Contrôles réguliers de la part des responsables hiérarchiques.
- Mécanismes de signalement anonymes.
- Définir clairement les positions hiérarchiques pour que le personnel sache à qui signaler ses préoccupations.
- Signalements/ reporting effectués par le biais d'une application.
- Entretiens de fin de contrat.
- Créer une culture positive autour du signalement/ reporting sur les incidents évités de justesse (par exemple, en comparant le reporting sur les incidents évités de justesse et les préoccupations, aux KPIs des responsables hiérarchiques).

Complément d'information

- ISOS Global Duty of Care Benchmarking Report, 2015
- CINFO Duty of Care Model

3.9 Lien avec la sauvegarde

Même si les définitions exactes et l'étendue de la sauvegarde peuvent différer selon les organisations, il existe plusieurs domaines où la sécurité et la sauvegarde s'alignent. Dans l'espace humanitaire, sauvegarder veut dire prévenir les dangers pesant sur les personnes et l'environnement, dans le cadre de la prestation de l'aide au développement et de l'aide humanitaire. Grâce à l'évolution de la sauvegarde dans le secteur, de nombreuses organisations incluent la protection de la santé, du bien-être, et des droits humains de tous les individus, avec une attention particulière aux communautés, pour qu'elles soient protégées des abus, des dangers, et des abandons.

Cela indique en effet le besoin continuel d'une collaboration étroite entre les fonctions de sauvegarde et de GRS.

Collaboration sur l'approche

Il est essentiel de reconnaître que les problèmes de sauvegarde peuvent se convertir rapidement en problèmes de sûreté et de sécurité pour tous les individus qui soumettent leurs inquiétudes à l'auteur présumé, et à ceux chargés d'enquêter.

L'opinion d'un expert

« Il n'existe pas de problèmes de sauvegarde qui ne soient pas des problèmes de sûreté et de sécurité ».
(Participant KII, Responsable de la stratégie GRS des ONGs)

Des campagnes ciblées et l'agression envers une organisation et son personnel peuvent rapidement dégénérer à cause d'une simple allégation à la sauvegarde. Intervenir dans des contextes, où il existe un manque d'accès à la surveillance, à l'évaluation et au signalement des problèmes de sauvegarde peut augmenter le risque, et requérir une approche plus intégrée et stratégique.

Kenya
Le personnel de ChildFund International visite un village rural au Kenya. Les membres du personnel doivent avoir clairement défini les rôles et les responsabilités GRS qui peuvent aussi inclure la sauvegarde des enfants.

Exemple dans ce secteur :

« En Somalie, le risque de recrutement de personnel trop jeune ou avec des antécédents criminels est toujours présent, et la vérification dépend, souvent, dans les zones rurales, de la relation entre la police locale et les responsables de la communauté.

Recruter dans ce contexte entraîne de nombreux problèmes, y compris des rivalités entre communautés, pour l'organisation avec laquelle j'ai travaillé. Nous avons dû équilibrer le nombre de personnes recrutées entre les différents groupes ethniques, car les chefs d'ethnies se présentaient au bureau s'ils pensaient qu'on les avait oubliés. Nous avons été alerté par le chef d'une communauté d'un cas d'offre d'emploi sexuel qui a déclenché le réexamen de la sauvegarde. Par ailleurs, le cas d'une femme, qui avait 18 ans, selon nos vérifications auprès de la communauté, mais qui selon les dires d'un membre du personnel n'avait que 16 ans. Nous avons donc été obligés de nous défendre contre des accusations d'exploitation économique d'une enfant.

Un autre membre du personnel avait apparemment dit à ses collègues qu'il était sur le point de se marier avec une fille de la communauté qui avait au maximum 13 ou 14 ans. Après avoir surmonté la résistance insistante de la communauté, nous avons pu parler à cette jeune fille qui a déclaré avoir 18 ans et qu'elle acceptait le mariage, mais apparemment, elle subissait des pressions de la communauté. Une formation additionnelle sur la sauvegarde a été mise en place grâce aux facilitateurs locaux, mais les cas de mariage à un âge précoce et d'offres d'emploi sont toujours présents ».

Participant KII, Responsable de la GRS opérationnelle des ONGs

D'un point de vue stratégique, les responsables de la GRS, de la sauvegarde, des RH, et des programmes doivent travailler en étroite collaboration afin de pouvoir garantir que les risques potentiels sont identifiés, que des mesures d'atténuation ont été convenues, et que les responsabilités ont été clarifiées en termes de prévention, de réaction, et de reprise. La compréhension du contexte de l'opération est primordiale dans cette relation, tout comme les fonctions nécessaires à l'atténuation de la sauvegarde et à l'escalade des risques de sécurité.

Les cycles de gestion des incidents de sauvegarde peuvent être légèrement différents selon les organisations. Mais il existe des points d'entrée grâce auxquels une relation solide entre la sécurité et la sauvegarde peut rationaliser les processus et permettre des résultats plus sûrs pour toutes les parties impliquées ainsi que le renforcement de la compréhension, et des approches éclairées de signalements des incidents.

Les formations en matière d'investigation sont un moyen d'assurer une collaboration plus étroite. Ces sessions doivent clairement mettre en évidence les rôles de l'organisation durant un incident de sauvegarde, s'assurer que les points focaux de la sauvegarde et de la GRS sont présents, et que toutes les parties suivent les protocoles clairement détaillés et basés sur des preuves. Il est nécessaire de garder à l'esprit que même si le personnel de GRS doit être informé, il est peu probable que cette équipe soit à même de gérer ou de diriger un incident de sauvegarde.

Dans certaines organisations, la frontière entre la sûreté et la sécurité est moins nette. Par exemple, la sauvegarde et la sécurité peuvent avoir le même point focal. Il n'existe pas qu'une seule façon de mettre en place cette relation ou de faire un meilleur travail, ceci dépendant des besoins et des attentes de l'organisation. Ce qui est important, c'est qu'une organisation comprenne bien les fonctions de la sauvegarde indépendamment de la sécurité, mais aussi leurs relations.

Complément d'information

- Safeguarding Resource and Support Hub
- GISF Webinar: Intersection of Security and Safeguarding (Webinaire du GISF : recoupement entre la sécurité et la sauvegarde)
- InterAction Blog: Launching the safeguarding community visual toolkit
- GISF 'How-to' Note On Implementing the safeguarding cycle (Note du GISF sur les modalités de mise en place du cycle de sauvegarde)

3.10 Lien avec l'équipe chargée des voyages

La gestion et le suivi des voyages du personnel dépendent souvent des demandes budgétaires. Les demandes sont souvent tributaires de la politique de Responsabilité sociale de l'entreprise (RSE), telle que la réduction des émissions de carbone. Cependant, la publication récente de l'Organisation internationale pour la normalisation (ISO), ISO 31030 : Gestion des risques liés aux voyages, indique clairement que le cas de la gestion des risques de sûreté et de sécurité doit être intimement lié au plan stratégique des voyages du personnel (international et national).

Gestion des risques liés aux voyages

ISO 31030 fournit des recommandations aux organismes sur la manière de gérer le ou les risques, pour l'organisme et ses voyageurs, lorsqu'ils effectuent un voyage.

Les fonctions de la GRS doivent s'engager dans le développement et le respect des bonnes pratiques en matière de gestion des risques liés aux voyages.

- Analyse du contexte et réunions d'information, pour déterminer quelle sources d'information utiliser, et comment elles sont présentées et communiquées.
- Autorisation et approbation, c'est-à-dire établir un système d'autorisation et d'approbation basé sur les évaluations des risques, les profils des voyageurs et des activités, en dehors des considérations financières.
- Suivi et surveillance des voyageurs, en sensibilisant l'ensemble de l'organisation sur les lieux où se trouvent les voyageurs en cas d'incident.
- Évacuation et relocalisation, en développant des plans d'urgence appropriés, adaptés au contexte.
- Développement de procédures standards de fonctionnement (SOPs), qui peuvent inclure des forfaits de dépenses par jour, et des politiques de sélection des transports et des logements qui tiennent compte de la gestion des risques de sécurité.
- Développement de procédures de planification des déplacements et des voyages dans le pays.

Complément d'information

- ISO 31010: 2021 Travel Risk Management: guidance for organisations (ISO 31010:2021 Gestion des risques liés aux voyages - Recommandations pour les organismes)

Madagascar
Un membre du personnel de World Central Kitchen se déplace à Madagascar pour aider à la distribution des repas après un cyclone. Tout déplacement de personnel doit toujours être encadré par des politiques de gestion des risques liés au voyage.

Chapitre 4 : Coordination, collaborations et partenariats stratégiques pour la GRS

En raison de l'ampleur des nouvelles menaces, englobant le changement géopolitique, les risques numériques et les cyberrisques, l'importance des collaborations en matière de sécurité au niveau stratégique est devenue essentielle. Il s'agit du renforcement des partenariats sectoriels, de la création de réseaux mondiaux, régionaux, et nationaux dédiés, de la formation de groupes de travail et du maintien de relations clés avec d'autres agences et organes officiels et non officiels. Ce processus est souvent effectif à un niveau opérationnel. Cependant, les organisations peuvent avoir des difficultés à formuler et à mettre en œuvre ces partenariats, réseaux, et groupes de travail de manière stratégique, en comptant sur le personnel des opérations pour construire une grande partie de ces relations, de manière formelle et informelle.

La norme ISO 31000:2018 Management du risque - Lignes directrices met en évidence l'importance de l'engagement des parties prenantes par le biais de la communication et de la consultation durant le processus de gestion des risques.

L'engagement des différentes parties prenantes au niveau opérationnel est déterminant pour le partage des informations de sécurité, l'évaluation des risques et la mise en place de mesures de sécurité efficaces. Cependant, l'absence de coordination et de collaboration au niveau stratégique avec différents acteurs, soutenus et guidés par des cadres supérieurs, expose le personnel à des risques supplémentaires. C'est encore plus important dans des environnements de travail complexes lorsqu'ils s'engagent avec des groupes armés non étatiques (NSAGs), et assurent la conformité avec la législation contre le terrorisme.

4.1 Collaboration interagences en matière de sécurité

Les organisations doivent s'engager dans le secteur et se coordonner avec les groupes humanitaires, de développement, et des droits de l'homme afin de partager leurs connaissances et expériences pour répondre aux menaces. L'engagement transversal entre les secteurs est fondamental pour assurer une bonne GRS. Il existe déjà de nombreuses instances opérationnelles et stratégiques pour la coordination nationale, régionale, et mondiale des ONGs de l'ONU, en matière de gestion des risques de sécurité, et des domaines parallèles. Notamment, le Groupe consultatif civil et militaire (CMAG), le Groupe de travail Global Access, l'accès à « Sauvons des vies ensemble » (SLT) du pays, et les groupes de travail sur la sécurité et les équipes humanitaires du pays.

Au cours des dernières années, les ONGs ont également formé différents réseaux et plateformes de sécurité au niveau du pays, au niveau régional et des sièges sociaux. Ces réseaux et plateformes de collaboration autour de la sécurité ont permis de faciliter l'échange des informations de sécurité, d'augmenter la sensibilisation à une bonne GRS grâce aux formations et aux ateliers et de promouvoir les bonnes pratiques entre les organisations.

Les organisations doivent chercher à formaliser de telles collaborations à un niveau stratégique et s'assurer qu'elles sont promues et comprises au niveau opérationnel afin de soutenir le personnel dans leur engagement et leur collaboration avec les organisations. Le Guide de collaboration pour les ONGs du GISF pour la sécurité fournit des conseils et des ressources pratiques pour aider les ONGs à collaborer à la sécurité de manière efficace avec d'autres organisations opérant dans le même contexte.

L'engagement et la collaboration entre les secteurs sont particulièrement importants pour les petites ONGs, les start-ups des pays, et les équipes de réponses aux situations d'urgence, puisqu'ils permettent un accès immédiat aux informations importantes qu'une organisation ne peut pas identifier par elle-même, à cause d'un manque de ressources. Il existe un grand nombre de barrières externes et internes à une collaboration efficace en matière de GRS, mais les organisations ont la nécessité de surmonter ces difficultés afin d'assurer une étroite collaboration.

Quelques réflexions importantes :

- ✓ Sensibilisation – Encourageons-nous le besoin de collaborer avec d'autres organisations ? Les avantages de la collaboration en matière de sécurité sont-ils bien compris dans l'ensemble des organisations ? Par exemple, le financement des donateurs institutionnels, et l'influence des cadres politiques sur les coûts directs/ indirects.
- ✓ Responsabilité – Notre personnel accepte-t-il d'être responsable du maintien des relations avec d'autres organisations ? Si les relations avec d'autres organisations ne sont pas gérées efficacement, comment pouvons-nous améliorer les choses ?
- ✓ Ressources – Avons-nous les ressources humaines et financières pour permettre à l'organisation d'être présente dans ces mécanismes de coordination ? Devons-nous envisager notre architecture de sécurité comme une organisation ? Avons-nous les systèmes appropriés en place pour la budgétisation de la sécurité ?
- ✓ Diversité des approches de sécurité – Les organisations ont des approches et des capacités de sécurité différentes, mais comment peuvent-elles apprendre les unes des autres ? Devons-nous comparer nos approches de la sécurité avec d'autres organisations opérant dans les mêmes environnements ?

Quelques réflexions importantes : *(suite)*

- ✓ Confidentialité – Les organisations n'aiment pas partager des informations sensibles pouvant les exposer à des risque supplémentaires. Quelles informations pouvons-nous partager et comment pouvons-nous les partager ? Construire des relations avec d'autres personnes durant- ou idéalement- avant les opérations de réponse aux situations d'urgence peut rapporter des dividendes parce que cela contribue à augmenter la confiance et l'échange mutuel d'informations.
- ✓ Priorités et contraintes de temps – Assister à des réunions sur la sécurité et s'engager avec d'autres organisations, consomme du temps et des ressources. Comment nous assurer que la collaboration pour la sécurité est une priorité et qu'elle soit envisagée comme un catalyseur qui enrichit et renforce la mise en application du programme ?

Répondre à ces questions peut conduire à un besoin d'assistance, de compétences supplémentaires et de ressources. Faire en sorte que les besoins explicites en collaboration, coopération et partenariats de votre stratégie GRS améliorent la capacité de l'organisation à long terme va promouvoir l'échange d'information et la coordination entre les organisations.

Voici un exemple concret de fonctionnement Cadre de « Sauvons des vies ensemble » (SLT) , établi pour la coordination d'une ONG de l'ONU. L'objectif de SLT est d'améliorer la capacité des organisations partenaires à prendre des décisions éclairées, à gérer les risques, et à mettre en place des dispositions de sécurité efficaces qui permettent d'aider, d'améliorer la sécurité du personnel, et la continuité des opérations. Inclure ces points dans votre stratégie GRS et demander au personnel de s'engager en conséquence.

Pour comprendre quels sont les organismes de coordination ou les opportunités de collaboration disponibles et importantes, les organisations doivent mener une analyse complète des parties prenantes en ce qui concerne la GRS. Cette analyse doit être conduite à un niveau stratégique, mais tenir compte des connaissances approfondies des organismes de coordination au niveau opérationnel avec lesquels le personnel est engagé, et des initiatives qui ont été mises en place. S'engager dans ce processus grâce à une approche participative permet aux organisations de développer des stratégies de coordination en matière de GRS qui lient les opérations mondiales aux opérations sur le terrain, et vice versa.

4.2 Collaboration et coordination interne

S'assurer que la stratégie GRS est mise en œuvre avec efficacité dans une organisation en engageant toutes les parties prenantes est un thème récurrent. Il ne s'agit pas seulement de discuter avec les membres du personnel opérationnel, mais de les inclure dans le processus. C'est-à-dire inclure le personnel opérationnel dans un groupe de travail sur la gestion interfonctionnelle des risques (voir le Chapitre 2) et les faire participer à la politique de développement. Dans cet optique, les organisations doivent :

- Évaluer régulièrement les besoins opérationnels – Prévoir des entretiens avec les informateurs clés (KIIs), planifier des réunions de GRS régulières, et trouver quels sont les risques les plus courants ou importants auxquels elles doivent faire face. Ces informations peuvent être utilisées pour influencer les priorités de GRS.
- Discuter des scénarios de la vie réelle – Faire en sorte que les scénarios soient proches des besoins quotidiens du personnel. Souligner comment la GRS peut leur permettre de mettre en place des programmes efficaces.

Une fois que les inquiétudes et les programmes ont été identifiés, il est vital de faire un suivi et d'établir les priorités.

- Communication et information – le personnel opérationnel sera plus actif s'il est tenu au courant des processus de l'organisation. Une approche transparente peut permettre au personnel de comprendre le développement des stratégies GRS. Ainsi, l'engagement et le soutien à la culture de la sécurité est plus important.
- Aligner la GRS de l'organisation avec la culture de l'attitude face au risque de l'organisation – Il s'agit de montrer comment la gestion des risques est intégrée à la stratégie, à la vision et aux objectifs de l'organisation, et comment elle renforce la stratégie organisationnelle et favorise la durabilité des programmes.

Considérations à prendre en compte lors de la mise en œuvre des politiques mondiales au niveau organisationnel

Il est nécessaire de prendre en compte de nombreux facteurs lors de la mise en application des politiques mondiales à un niveau régional ou national. Si le personnel opérationnel n'est pas- ou peu impliqué- lors de l'introduction de nouvelles politiques, des difficultés sont à craindre :

- Contexte – Les organisations travaillent souvent dans plusieurs régions dont l'environnement est considérablement différent pour chacune. Il n'existe pas de procédure « à taille unique » dans une organisation.
- Appropriée au plan culturel – Du point de vue culturel, les gens ont une approche différente de la gestion des risques, qui va souvent de pair avec l'environnement dans lequel ils vivent et qui est donc intuitive.

- Technologie – Dernièrement, les organisations ont pensé à des solutions technologiques. Notamment, des applications mobiles qui envoient des communications de groupe ou fournissent un suivi et des alertes de sécurité. Sont-elles accessibles au personnel de l'organisation ? L'organisation les finance-t-elle de manière appropriée et procure-t-elle les ressources appropriées ?
- Langage – Le langage en matière de GRS peut être complexe et technique. Le personnel dont l'Anglais est la deuxième langue peut rencontrer des difficultés avec la terminologie. La simplicité est l'une des clés de la GRS. Il est primordial que les spécialistes de la GRS adoptent un langage que les autres puissent comprendre plutôt que leurs auditeurs essaient de comprendre le langage de la GRS. La GRS est un facilitateur, elle doit donc faire ce qu'il faut pour gagner des adhésions et des appuis, et ainsi parvenir à des communications plus efficaces et précises.

Exemple dans ce secteur :

« Mon organisation a réellement élaboré de bonnes stratégies et politiques pour améliorer la GRS, mais elle n'a pas pris en compte les réalités sur le terrain. Le personnel ne sait pas lire l'Anglais, la connexion Internet n'est pas fiable dans nos bureaux locaux, les systèmes basés sur les applications sont donc inappropriés. Nous avons aussi essayé d'expliquer pendant plusieurs mois que la politique de sauvegarde introduite, n'était pas applicable à notre contexte ».

Participant KII, Directeur pays au Moyen-Orient

4.3 Développement de la politique de partenariats

Dans le cadre du développement de partenariats avec d'autres ONGs, les agences de l'ONU et les donateurs, il est crucial d'avoir une compréhension globale de la stratégie GRS de l'organisation. C'est-à-dire, une bonne compréhension de l'approche des risques de l'organisation et de ses politiques de travail en partenariat, y compris une description et une limitation claires des responsabilités en ce qui concerne le devoir de diligence.

Les partenariats peuvent prendre différentes formes : internationaux, nationaux et locaux, associations membres ; partenaires de mise en œuvre externes ; et de plus en plus la forme de consortiums. Le guide d'action conjointe des partenaires du GISF fournit des conseils détaillés sur l'établissement équitable de partenariats entre les ONGs internationales et les ONGs locales ou nationales.

Ce guide procure de nombreux outils et conseils sur la formalisation de la GRS dans le cadre des partenariats. Cependant, les organisations doivent aussi instaurer une politique ou une position mondiale sur la formation des partenariats. Une politique interfonctionnelle qui aborde toutes les questions du devoir de diligence, notamment la sécurité.

À un niveau basique, les partenariats doivent être en phase avec la stratégie de l'organisation. Il est également important de se demander pourquoi des partenariats sont formés. Sont-ils mis en place pour localiser l'aide humanitaire ou pour minimiser les risques pesant sur l'organisation ? Dans le dernier cas, les risques sont-ils transférés aux partenaires ou partagés avec les partenaires ?

Le transfert du risque se rapporte au déplacement complet du risque d'une partie à l'autre, ce qui est souhaitable dans certaines circonstances, si le risque est complètement transparent, identifié et accepté par les deux parties. Cependant, pour que le partage du risque soit véritable, les deux parties doivent comprendre les risques auxquels chaque partie est exposée, accepter les risques dans les mêmes termes d'égalité, sans déséquilibre des pouvoirs, et que les ressources pour les résoudre soient équitablement allouées.

Meilleures astuces : Donateurs et risques

Les donateurs peuvent aussi poser des questions sur les risques et les partenariats, en particulier s'ils transfèrent complètement les risques. La pression des donateurs est l'une des réponses les plus fréquentes lorsqu'il s'agit de prendre des risques inutiles. Les donateurs doivent donc aussi comprendre les niveaux de risque que vous êtes disposé(e) à prendre.

Comme cela est indiqué dans le document de recherche du GISF Partenariats et gestion des risques de sécurité : point de vue des partenaires locaux, il est crucial pour les ONGs de voir les partenaires, selon le point de vue des ONGs locales, avec lesquelles ils travaillent.

La réussite des partenariats requiert la création, le transfert, et le partage des risques de sécurité entre les partenaires. Pour cela, il est nécessaire que les deux organisations partenaires aient une compréhension détaillée des problèmes de sécurité, et que vous sachiez comment, en tant que partenaire solidaire, vous pouvez travailler ensemble pour améliorer globalement la sécurité dans toutes les organisations concernées.

Un autre problème commun au personnel opérationnel auquel le personnel au niveau stratégique ne peut quasiment jamais répondre est . quel est mon devoir de diligence envers nos partenaires ? Pour répondre à cette question, l'approche du devoir de diligence doit être documentée comme nécessaire, et le personnel doit être aidé. Dans cette optique, les questions suivantes doivent être prises en compte :

Questions sur le partenariat en gestion des risques de sécurité (lien avec votre stratégie GRS)	
Devoir de diligence	Quel notre devoir de diligence légal et moral envers nos partenaires ? La réponse doit être indiquée dans les paramètres de protection que l'organisation doit fournir.
Gouvernance et responsabilisation	Quelle norme de GRS attendons-nous de la part de nos partenaires ? Comment allons-nous pouvoir la mesurer ? Les accords de partenariat vont-ils pouvoir étayer la GRS ?
Transfert de risque versus partage du risque	Allons-nous transférer tous les risques et la responsabilité de la gestion des risques aux partenaires ou allons-nous partager les risques avec les partenaires ?

Questions sur le partenariat en gestion des risques de sécurité (lien avec votre stratégie GRS) *(suite)*	
	Sommes-nous d'accord pour que nos partenaires prennent plus de risques que notre personnel ? Si oui, de quel niveau de risque parlons-nous ? Quel soutien devons-nous fournir pour les aider à gérer ces risques ? Sommes-nous disposés à augmenter l'aide à nos partenaires en fonction du niveau de risque ? Si oui, quel type de support doit-on fournir?
Politiques et principes	Nos partenaires doivent-ils s'aligner sur nos principes humanitaires et politiques spécifiques ?
Gestion des incidents critiques	Quelle aide devons-nous fournir à nos partenaires en cas d'incident critique ? Doit-elle être différente de l'aide que nous procurons à notre personnel ?
Fin d'un partenariat	Quelle est l'étendue de notre devoir de diligence envers nos partenaires à la fin d'un accord de partenariat ?

La gestion des partenariats et de la diligence raisonnable est un processus complexe, mais qui doit être aligné sur la stratégie et les valeurs organisationnelles. C'est pourquoi, pour assurer la cohérence dans tous les partenariats, les politiques qui présentent le devoir de diligence doivent être absolument communiquées aux partenaires, et contrôlées au niveau stratégique (voir également la section 3.8 Lien avec le domaine légal).

Complément d'information

- ISO 31000:2018 Risk Management Guidelines (ISO 31000:2018 Management du risque - Lignes directrices)
- GISF Co-ordination for Humanitarian Security Management (GISF - Coordination pour la gestion de la sécurité humanitaire)
- GISF Collaborative Security Risk Management: A case for local development (Gestion collaborative des risques de sécurité du GISF : un dossier pour le developpement local)
- UN Saving Lives Together Framework
- GISF Partnerships and Security Risk Management Joint Action Guide (Guide GISF pour une action conjointe de gestion des risques de sécurité et pour les partenariats)

Chapitre 5 : Contribution de la GRS à résilience organisationnelle et à la continuité des activités

Pour être résiliente, une organisation doit être préparée à l'adversité, être capable de répondre aux perturbations et aux crises, et de réagir efficacement et positivement en présence de conditions difficiles. Les organisations humanitaires et de développement se retrouvent souvent dans l'obligation d'agir dans des environnements de plus en plus politisés, ne sont plus perçues comme politiquement neutres, et doivent se contenter d'espaces civiques plus restreints. L'ampleur et la fréquence des crises auxquelles sont confrontées les organisations sont sans précédent. Les stratégies organisationnelles doivent reconnaître et aborder le lien entre les risques en matière de sécurité et de sûreté, la continuité des activités et la résilience organisationnelle. Toutes les organisations doivent disposer de mécanismes complets en place pour répondre et résister aux changements, parfois imprévisibles, des contextes opérationnels et des événements critiques.

5.1 Préparation et planification

Les professionnels de la GRS doivent participer aux réunions de préparation et de planification des organisations. La résilience pour les organisations, les équipes, et les individus doit être définie et référencée dans les politiques concernées de GRS, parallèlement aux mesures pratiques sur les modalités de support prodiguées par la GRS à l'organisation toute entière, au cours des discussions sur la planification de la préparation, et de la réponse. La sûreté et la sécurité jouent un rôle important dans les situations traditionnelles de réponse à la crise, aux incidents frauduleux, au risque de réputation, à la sauvegarde ou aux pandémies mondiales.

Venezuela

Un travailleur humanitaire prend la température d'une famille durant la pandémie de Covid-19. Les organisations doivent disposer de mécanismes pour adapter leurs procédures de sécurité aux événements critiques, comme les urgences de santé publique.

OCHA/Gema Cortes

Définitions clés :

- **Continuité des activités :** La planification stratégique et procédurale qu'une organisation met en place pour garantir que ses fonctions essentielles se poursuivent pendant et après un événement perturbateur.
- **Crise :** Un événement ou une série d'événements, qui perturbent notablement les opérations normales, en causant ou en pouvant causer de graves conséquences qui ont un impact sur l'organisation toute entière. En général, une crise demande une réponse qui va delà des mécanismes de gestion normaux pour traiter l'impact et ses répercussions.
- **Incident critique :** Un événement indésirable qui se traduit ou peut se traduire en préjudices graves pour le personnel, en une perturbation des programmes et des activités ou en une perte ou des dommages sur les biens de l'organisation ou sa réputation, mais qui est gérable dans le cadre du protocole normal avec le soutien du siège social.
- **Incident :** Un incident est habituellement géré seulement pas les individus situés dans les pays ou à proximité du site où l'incident a lieu ou a eu lieu.
- **Résilience organisationnelle :** Il s'agit de la capacité de l'organisation à anticiper, résister, répondre, et à se rétablir des menaces, des incidents ou des perturbations ayant mis en danger sa sécurité, tout en conservant ses fonctions essentielles, sa réputation et la confiance des parties prenantes.

Préparation des crises relatives à la GRS ou des crises impliquant la GRS

Le succès de la résolution et de la gestion des situations de crise dépend de la capacité de l'organisation à prendre des décisions appropriées rapidement. Ceci requiert une préparation, un bon flux d'informations et des canaux de communication clairs que tout le personnel comprenne. Même si toutes les crises sont différentes et qu'il n'est pas possible de prévoir toutes les éventualités, il est possible de planifier comment répondre à chaque crise avec efficacité en laissant à l'organisation des disponibilités suffisantes pour continuer à fonctionner sans utiliser toutes ses ressources pour résoudre un événement. Une approche stratégique organisationnelle de la gestion de la crise et de la continuité des activités joue un rôle important dans l'allocation des ressources nécessaires à la GRS pour préparer et répondre aux événements perturbateurs.

La préparation et la planification varient en fonction de l'organisation et des différentes fonctions stratégiques. Par exemple, les organisations intervenant dans des environnements propices aux conflits sont plus à même de développer un cadre pour une prise de décision éclairée en termes de risque, d'investir des ressources dans la construction d'installations plus sécurisées, de déployer un personnel formé à la sécurité, et d'établir des partenariats et des mécanismes stratégiques pour mieux coordonner leurs réponses à la crise. Par ailleurs, les

organisations intervenant principalement dans des contextes à risques modérés peuvent se permettre de moins investir dans leur infrastructure ou de revoir leurs plans de gestion de crise périodiquement ou de faire des prévisions à la faveur d'élections ou de dangers climatiques saisonniers. Les deux contextes présentent des risques qui sont une véritable menace pour les opérations de l'organisation, il est donc vital que la GRS et la préparation ne soient pas envisagées seulement du point de vue de la sûreté et de la sécurité.

La préparation stratégique de l'organisation peut prendre la forme d'évaluations complètes des risques, de planification d'un scénario stratégique, d'allocation de ressources pour faire face au risque, de formations et d'améliorations continues. Les responsables de la GRS peuvent également mettre en place une évaluation des besoins en formation pour l'organisation toute entière, offrant des opportunités au personnel de se qualifier opportunément, et de renforcer la capacité de l'organisation.

5.2 Approche interfonctionnelle de la gestion de crise

Une approche interfonctionnelle est importante pour réussir la gestion d'une crise affectant votre organisation, personnel et/ou biens. En présence d'une crise, l'obtention d'un bon résultat dépend du travail collaboratif de l'équipe interfonctionnelle ; collaborer et communiquer pour atteindre un but commun : la résolution d'une crise. La collaboration interfonctionnelle doit être cultivée et développée avant la crise, plutôt que pendant que l'on essaie de faire face à la crise.

Interfonctionnalité durant la réponse à une crise

Malgré l'importance d'identifier un responsable d'équipe chargé de la gestion de crise (en général, les organisations désignent leur PDG, Directeur des opérations ou un Directeur qui a une grande expérience et des connaissances en gestion de crise dans le cadre institutionnel), toutes les fonctions représentées dans une équipe de gestion de crise sont autorisées à passer à l'action, ont des rôles et responsabilités interdépendants, mais néanmoins bien définis. Les responsables de la GRS doivent être accueillis avec la même considération que les représentants d'autres fonctions au sein de l'équipe.

Sri Lanka
Les participants procèdent à un exercice de recherche et de sauvetage dans l'éventualité d'une d'inondation. La formation est indispensable afin que tous les membres de l'équipe soient en sécurité lorsqu'ils travaillent dans des environnements à haut risque.

Le tableau ci-dessous présente les relations interfonctionnelles dans une équipe de gestion de crise.

Risques de cybersécurité Sécurité numérique Conformité au RGPD	Réservations de voyages Conditions d'obtention d'un visa Kit sécurité de voyage et poste de santé (trousse de premiers secours, téléphones satellites)	Devoir de diligence/ obligations légales Devoir de diligence Exigences contractuelles Protocolo de acuerdo
Agent de liaison avec les familles Formulaire de renseignements sur la famille Certificat de vie	Fonds pour pallier les urgences Avances en argent liquide	Communications internes Déclarations externes/ à la presse Communications de crise
Emplacement du personnel Procédures d'enregistrement	Gestion du budget du projet	Gestion des parties prenantes externes

Exemple d'une interfonctionnalité durant la réponse à une crise International Location Safety

Continuité des activités

Les crises sont des incidents qui ne peuvent pas être gérés selon des mesures et des processus de routine. En tant que telles, il est important pour les organisations d'intégrer dans la conception de leur gestion de crise et/ou des plans de continuité des activités, la mesure dans laquelle elles pourront continuer à répondre aux exigences normales en cours pendant que leurs responsables sont occupés à répondre à un incident majeur. Une résilience organisationnelle efficace requiert à tous les responsables de fonctions, y compris la sécurité, d'assurer qu'il y a suffisamment de ressources, de compétences et de capacités pour l'entretien des fonctions et des opérations principales de l'organisation, et qu'elle est en mesure de continuer à délivrer ses prestations de service durant ou après une crise.

Complément d'information

- GISF NGO Crisis Management Exercise Manual (Manuel d'exercice du GISF pour la gestion de crise des ONGs)
- GISF Crisis Management of Critical Incidents (GISF - Gestion de crise des incidents critiques)
- Frontline Defenders Handbook

UN OCHA/Matteo Minasi

Haïti

Des agents humanitaires coordonnent leur réponse après un tremblement de terre. Les organisations doivent tenir compte de l'éventualité de crises plus importantes dans leurs plans afin de savoir comment elles réagiront et pourront continuer à fonctionner normalement.

Chapitre 6 : Suivi, évaluation, redevabilité et apprentissage (MEAL)

6.1 Pourquoi MEAL est important – concepts de base

La clé du succès d'une stratégie GRS est d'établir des processus pour le sulvi et l'évaluation de son efficacité, et à terme de son impact. La mise en place d'une stratégie GRS globale requiert une évaluation et une adaptation continues. C'est pourquoi, un système MEAL global, va permettre d'obtenir qualité et amélioration continues, efficacité et résultats, dans le processus. Un système MEAL intégré permet aussi à l'organisation de mesurer à quel point la stratégie GRS contribue à- ou soutient- la réalisation d'objectifs organisationnels plus étendus.

Définitions clés :

- **Théorie du changement :** Une explication complète sur les modalités et les causes du désir de changement qui est supposé se produire dans un contexte particulier. Elle indique la voie à suivre pour obtenir tous les résultats. Elle propose tout d'abord de mettre en évidence les résultats souhaités à long terme et de travailler pour identifier toutes les conditions (sous-résultats) qui doivent être mises en place (et comment elles sont reliées de cause à effet) pour l'obtention des résultats.
- **Cadre logique (Logframe) :** Un cadre logique est un tableau ou une matrice qui fait la liste des activités au programme, des résultats à court et à moyen termes, et des objectifs à long terme. Il indique comment la logique des activités va permettre d'atteindre les résultats, et au final l'objectif. Il inclut les indicateurs utilisés pour mesurer les progrès, la source des données, et les actions nécessaires pour mener à bien le projet.
- **Plan MEAL :** Un document synthétique sur les modalités de réalisation des plans de suivi et d'évaluation, y compris une liste de ce qu'il faut mesurer et pourquoi, des activités clés, des budgets, des responsabilités et des délais.

Déterminer comment suivre et évaluer les systèmes GRS, définir les exigences de reporting pour les personnes redevables, et préciser comment l'apprentissage doit être partagé, nécessite de l'expérience dans le suivi, les techniques, et les pratiques d'évaluation. Il est donc fortement recommandé que les responsables de la stratégie de GRS travaillent en collaboration avec les spécialistes techniques du MEAL dans leur organisation, afin de développer le processus qui fonctionne le mieux pour eux.

Meilleures astuces : Huit raisons d'inclure un plan MEAL dans votre stratégie GRS

1. Permet d'utiliser des systèmes, des politiques, et des procédures plus solides et intuitifs.
2. Indique dans quelle mesure les objectifs stratégiques et les résultats désirés sont atteints.
3. Garantit que l'argent et les ressources sont dépensés de manière efficiente et efficace.
4. Fournit des données précises qui peuvent être utilisées pour les communications internes et externes, les applications de financement, les donateurs ou le reporting pour le conseil d'administration
5. Peut être intégré dans le planning de gestion de crise et de continuité des activités pour identifier les lacunes et les menaces.
6. Permet une approche dynamique et adaptative pour une mise en œuvre pratique des stratégies de sûreté et de sécurité.
7. Donne la parole au personnel, aux clients, et aux parties prenantes.
8. Augmente la motivation et l'attention des personnes chargées de mettre en place la stratégie de sûreté et de sécurité.

6.2 Développer un plan MEAL

Un plan MEAL permet de communiquer votre approche et de mettre en relief les moyens d'atteindre vos objectifs, d'indiquer qui est responsable, et quels sont les financements/ ressources nécessaires. Il permet de souligner les responsabilités (redevabilités), l'apprentissage et au final d'améliorer votre crédibilité, il favorise une compréhension commune de vos objectifs (voir L'outil 12 : Exemple de Plan MEAL).

Meilleures astuces : Créer une Théorie du changement et un plan MEAL efficaces

- ✓ Démarrer en ayant l'objectif final en tête : définir vos objectifs à long terme.
- ✓ Être précis(e) et réaliste en choisissant les indicateurs, et s'assurer qu'ils sont SMART (spécifique, mesurable, atteignable, pertinent, et limité dans le temps).
- ✓ Déterminer les étapes pour identifier les résultats à court, moyen, et à long termes.
- ✓ Impliquer vos parties prenantes (voir la section 6.3) afin de garantir leur engagement, retour d'information et contribution au processus, elles devront faire en sorte que le processus fonctionne.
- ✓ Contextualiser vos objectifs. La façon dont le changement se produit peut être différente pour une équipe travaillant dans un pays à haut risque avec un régime répressif à un seul parti, par rapport à une équipe travaillant dans un contexte à faible risque dans une démocratie avec plusieurs partis. Adapter vos indicateurs au contexte dans lequel ils sont utilisés.
- ✓ Examiner et revoir votre modèle de théorie du changement pour l'adapter à ce qui fonctionne ou ne fonctionne pas, et aux changements dans votre stratégie ou environnement opérationnel.

6.3 Suivi routinier des progrès de la GRS

Sélectionner les indicateurs de GRS

Les indicateurs peuvent être quantitatifs, tels que le nombre de signalements d'incident de sécurité, de formations en sécurité ou de personnel formé. Ou ils peuvent être qualitatifs, et porter sur les préoccupations, les commentaires ou les expériences des personnes. Si vous pouvez obtenir et utiliser des données pour illustrer votre parcours, vous réussirez à avoir de l'impact.

Chaque indicateur doit être :

- Directement lié au rendement, résultat ou objectif indiqué dans la théorie du changement.
- Doit pouvoir être mesuré avec précision, en utilisant des méthodes qualitatives et quantitatives ou des méthodes mixtes et vos ressources disponibles.

Sélectionner des points de données de GRS

Il existe des exemples de points de données de GRS spécifiques qui peuvent être introduits dans les indicateurs sur mesure, et utilisés pour souligner aussi bien les changements positifs que négatifs.

- Incidents signalés
- Préoccupations signalées ou incidents évités de justesse
- Mesure de l'engagement ou utilisation des canaux de signalement.
- Commentaires sur la sûreté et la sécurité extraits des rapports concernant les programmes.
- Rapports sur les commentaires issus des entretiens en face en face et des entretiens de fin de contrat ou des questionnaires.
- Études de perception qui mesurent la conscientisation.
- Compréhension et participation aux politiques et procédures de GRS.
- Participation aux formations (interne et externe).
- Présences et minutes du point focal des réunions sur la GRS ou la sécurité.
- Journaux des voyages/ déplacements internationaux.
- Déclarations aux assurances.
- Dépenses actuelles et futures en ressources GRS.
- Comparaison et évaluation par rapport aux normes externes.
- Audits internes concernant :
    - Élaboration et vérification des documents de GRS (plans de gestion de la sûreté et de la sécurité,
      évaluations des risques, plans de gestion des incidents, rapports sur la sécurité, procédures sur la sûreté et la sécurité durant les voyages).
    - Bureau des contrôles et des enregistrements portant sur la sûreté et la sécurité.
    - Contrôles ou enregistrements concernant la sécurité des véhicules.
    - Journaux des déplacements et voyages du personnel national.

6.4 Évaluation

Pouvoir quantifier et mesurer le changement culturel et social de manière tangible peut constituer un outil essentiel pour communiquer la valeur et l'efficacité de l'investissement en GRS. Il n'existe pas de méthode ou d'approche utilisée pour mesurer ou évaluer l'impact. Il y a bien une approche qui consiste à utiliser un modèle de théorie du changement (ToC) qui cartographie les liens entre vos apports, vos activités, vos résultats, et comment tous ces éléments peuvent aboutir aux résultats et à l'impact recherchés.

Les modèles de ToC les plus efficaces sont simples et se concentrent sur :

- Le problème que votre cadre de GRS tente de résoudre (par exemple, un manque de prise de conscience et d'engagement en GRS, un accroissement des menaces faites au personnel)
- L'impact que vous essayez d'obtenir (par exemple, la création d'un environnement sûr et sécurisé pour tous ceux qui travaillent pour- et au nom de- votre organisation)
- Les conditions requises pour atteindre ces résultats (voir L'outil 10 : Diagramme simple de ToC).

6.5 Redevabilité

L'engagement de l'organisation est une condition essentielle à la construction d'une culture brillante de GRS. C'est pourquoi, il est primordial d'associer des responsables, des fidéicommissaires, et des collègues, dans les processus d'apprentissage MEAL, et d'être transparent en ce qui concerne la redevabilité, si les objectifs n'ont pas été atteints. Par exemple, incorporer la GRS aux KPIs des rapports trimestriels du conseil d'administration peut assurer une bonne intégration de la GRS, en l'associant clairement au succès de l'organisation.

Disposer de systèmes d'audit et de conformité appropriés en place à tous les niveaux de l'organisation, permet de lire clairement les résultats et de prendre des sanctions si la conformité n'est pas respectée. Des définitions claires des responsabilités et des actions spécifiques pour la conformité doivent également être énoncées dans le cadre logique pour assurer une redevabilité complète.

Exemple dans ce secteur :

« Notre organisation avait de bons systèmes et processus écrits en place pour la GRS, cependant, ils n'ont jamais été suivis ni vérifiés correctement. Des politiques avaient bien été transmises, mais sans faire l'objet d'un suivi ou d'une prise en charge des répercussions au cas où une évaluation des risques ou un plan de gestion des incidents n'auraient pas été achevés. Aucun forum ou mécanisme de vérification n'avait été établi pour le partage ou la vérification de la mise en œuvre des politiques. On pensait simplement qu'une fois la politique transmise, il suffirait que le personnel la mette en application, sans nécessiter grand soutien des cadres supérieurs stratégiques de l'organisation ou du suivi des progrès ou de l'impact ».
Participant KII, Responsable opérationnel des ONGs

6.6 Apprentissage

Les stratégies les plus réussies de GRS sont celles qui sont constamment révisées, adaptées et corrigées avec des opportunités constantes de réflexion et d'apprentissage collectifs, structurés, et/ou informels.

L'opinion d'un expert

« Nous n'avons jamais collecté de données dans le but d'obtenir des données. Nous ne recueillons que les données que nous allons utiliser lors de nos réflexions et révisions ».

(Participant KII, Responsable stratégique des ONGs)

C'est une bonne pratique de partager les apprentissages à tous les niveaux, positifs comme négatifs, car elle renforce la redevabilité et la transparence et encourage une approche plus participative.

L'opinion d'un expert

« Nos points focaux de sécurité se rencontrent régulièrement pour discuter des problèmes de sûreté et de sécurité importants avec leurs directeurs pays, qui divulguent ensuite les informations clés à tout le personnel et dans toutes les réunions dédiées au personnel ».

(Participant KII, Directeur international S&S des ONGs)

Le processus d'apprentissage doit fonctionner dans les deux sens. Il inclut un processus de transfert visant à renforcer le partage des informations de GRS provenant des responsables stratégiques (c'est-à-dire l'assimilation d'un nouvel apprentissage) dans l'ensemble de l'organisation. Par ailleurs, il inclut un processus de commentaires participatif qui utilise ce qui a été appris et définit des actions claires en fonction des leçons apprises.

Soutenir ainsi l'apprentissage dans l'organisation, permet de construire une culture de GRS gratifiante et auto-suffisante. En suivant ce processus, les organisations peuvent préparer une ouverture au changement qui, au final, renforce le renouvellement stratégique.

Meilleures astuces : Bons mécanismes d'apprentissage

- Cartographier le flux des connaissances. Qui a accès et à quelles informations ? Qui n'a pas accès aux informations positives ? Qui sont les gardiens des connaissances ? Comment pouvez-vous partager facilement ces connaissances en interne et avec l'extérieur ?
- Impliquer l'équipe de cadres supérieurs dans le processus. Mettre en évidence les atouts et souligner le potentiel inexploité.
- Réfléchir aux points forts de votre organisation et souligner les domaines qui doivent être améliorés.
- Optimiser les périodes de changement. Les changements organisationnels peuvent être stressants, mais ils peuvent aussi fournir des opportunités pour jeter les bases de nouvelles façons de travailler.
- Rechercher des moyens agiles de capturer les connaissances. Organiser des réunions avec l'équipe et avec toutes les équipes, et penser aux publics potentiels pouvant maximiser le potentiel des informations.
- Créer des ressources dans des sites accessibles et diriger les personnes vers ces sources à chaque fois que c'est possible.

Wilsdon, N. Institute of Voluntary Action Research, 'Taking a strategic learning approach to evaluation'

6.7 Méthodes de collecte des données

En développant un plan MEAL, une organisation doit tout d'abord déterminer les éléments qu'elle souhaite suivre. La priorité est ensuite de sélectionner vos méthodes de collecte des données. Il existe un grand nombre d'outils et de méthodologies quantitatifs et qualitatifs pour les choisir. Ces méthodes peuvent être utilisées en tandem ou en association en fonction du budget, des objectifs, et du temps dont dispose votre organisation. Ces techniques peuvent changer, mais elles donnent toutes l'opportunité aux équipes GRS de vérifier régulièrement et méticuleusement le niveau d'efficacité de la stratégie GRS. Il ne s'agit pas seulement de dépenser de l'argent, et que les ressources soient investies de manière efficace, mais aussi de permettre des corrections, des adaptations et des commentaires sur l'approche stratégique.

Un résumé des exemples d'outils de collecte est fourni ci-dessous.

Type d'outils	Les pour	Les contre
Surveillance routinière	Fournit des données à jour et permet de prendre des mesures correctives.	
Enquête	Permet de collecter des données d'un grand nombre de personnes. Très polyvalentes : les enquêtes peuvent être conduites en ligne, par téléphone ou en personne, et recueillir aussi bien des réponses quantitatives que qualitatives.	Il peut être difficile de vérifier l'étendue de la relation de cause à effet entre deux ou plusieurs éléments.
Entretiens	Permettent une discussion plus approfondie sur un sujet. Entretiens structurés ou semi-structurés qui fournissent l'opportunité d'adapter les conversations aux besoins, et une certaine flexibilité pour répondre aux participants. Utiles pour les sujets sensibles.	Les réponses peuvent être influencées par la partialité de l'interviewer (si ses convictions ou ses attitudes influencent les réponses des répondants) ou la désirabilité sociale (si un répondant fournit les réponses qu'il pense que l'interviewer veut entendre). Consommation de nombreuses ressources et chronophage. Plus difficile de produire des données quantifiables
Groupes de discussion	Convient pour acquérir une compréhension plus approfondie d'un problème ou d'un point de vue, et partager des commentaires et des apprentissages.	Analyse chronophage. Les participants, dont la personnalité est plus effacée, pourraient ne pas donner leur opinion.
Étude de cas	Idéale pour avoir une idée détaillée d'un sujet spécifique, d'un groupe, d'un individu ou d'un programme.	Difficile de généraliser les observations ou les conclusions. Risque de partialité, les chercheurs peuvent essayer d'utiliser les études de cas pour valider leurs hypothèses plutôt que de fournir des preuves objectives à un problème.

Type d'outils	Les pour	Les contre
Audits en face à face	Permet de recueillir des informations dans un contexte plus naturel, ce qui peut donner des résultats plus précis.	Les audits planifiés peuvent empêcher les participants d'avoir un comportement naturel. Les études observationnelles sous couverture, ne fournissent pas aux participants l'opportunité de consentir à participer.
Journaux sur la sécurité/ base de données sur les incidents de sécurité	Suivi uniforme des préoccupations en matière de sécurité et de sûreté, des incidents et des incidents évités de justesse, et de ce fait idéal pour les signalements officiels.	Doit être à la portée de tout le personnel. Requiert une bonne culture du signalement, pour que le signalement soit envisagé sous un angle positif.
Indicateurs de performance clés/ de satisfaction	Peuvent être qualitatifs ou quantitatifs. Concernent des objectifs/ domaines spéciaux de l'organisation. Favorisent la responsabilisation.	Doivent être associés à d'autres méthodes de manière à ne pas être envisagés comme des mécanismes punitifs.
Audits annuels (internes ou tierces parties)	Fournissent une analyse complète des connaissances, du comportement et des pratiques de GRS dans un contexte donné, et peuvent évaluer les opérations par rapport aux normes minimales de sécurité opérationnelle.	Peuvent être chers et requièrent des ressources additionnelles.

Complément d'information

- Oxfam's Participatory Capacity and Vulnerability Analysis: A practitioner's guide
- The World Bank: M&E; Some Tools, Methods and Approaches
- Overseas Development Institute: Supporting Adaptive Management
- INTRAC: M&E Universe
- Bond UK: Choosing Appropriate Evaluation Methods

Boîte à outils de la GRS

Outil 1
Développer vos orientations stratégiques – Exemple

Orientation stratégique 1 : Approche organisationnelle de la GRS

Résultat : Toutes les parties prenantes sont sensibilisées à l'approche organisationnelle du risque et connaissent les seuils de risque.

N°	Objectif	Qui est responsable	Date d'échéance	Mesures pour réussir
1.1	Définir l'attitude face au risque et les seuils de risque	Équipes exécutives	Fév. -26	* Déclaration d'attitude face au risque développée et déployée à tout le personnel. * Matrice de seuil de risque complétée et communiquée à tous les responsables stratégiques.
1.2	Confirmation de l'approche stratégique de la GRS	Directeur international de la GRS et Comité de gestion des risques	Déc-27	* Analyse contextuelle de toutes les opérations pays et des activités terminées. * Les équipes des programmes et de GRS s'accordent sur une approche d'acceptation, de protection et de dissuasion dans chaque contexte/ programme opérationnel. * Approches incluses dans la formation interne.

Orientation stratégique 2 : Augmenter la conscientisation

Résultat : Toutes les parties prenantes prennent conscience et acceptent leurs rôles et responsabilités en ce qui concerne la réduction des risques humains, des risques liés à l'information et aux biens physiques.

N°	Objectif	Qui est responsable	Date d'échéance	Mesures pour réussir
2.1	Promouvoir la compréhension de la GRS aux niveaux fonctionnel, opérationnel et stratégique de la GRS grâce à un programme de prise de conscience interne structuré.	Département de la GRS	Déc-27	* Programme interne de sensibilisation à la GRS développé et déployé à tout le personnel. * Examen semestriel des pratiques de gestion des risques suivies par les différentes parties prenantes (par exemple, le signalement d'un incident, le développement des évaluations des risques/ des outils de gestion des risques).
2.2	Fourniture d'une formation interne et externe à la sûreté et à la sécurité (selon la matrice de formation).	Directeur international de la GRS et Comité de gestion des risques	Déc-27	* Vérification annuelle du niveau de participation à la formation sur la sûreté et la sécurité. * Vérification trimestrielle du niveau de satisfaction sur la formation fournie.
2.3	Structure de gouvernance en place relative à la GRS.	Équipes exécutives	Fév. -26	* Structure de gouvernance adoptée, rôles et responsabilités assignés à chaque niveau. * Processus de recrutement du personnel confirmé. * Structure de gouvernance communiquée à tout le personnel.

Orientation stratégique 3 : Culture de la sûreté et la sécurité

Résultat : La culture de l'organisation et l'approche des programmes et de la réalisation des objectifs organisationnels est étayée par la conscientisation à la sûreté et à la sécurité. La gestion des risques de sécurité est une partie clé du processus de planification.

N°	Objectif	Qui est responsable	Date d'échéance	Mesures pour réussir
3.1	Inclure la GRS dans les étapes de planification des activités opérationnelles.	Département de la GRS	Déc-27	* La GRS apparaît régulièrement dans les points de l'ordre du jour et des minutes. * Les processus de planification incluent l'engagement/ l'approbation de la GRS.

3.2	Définir 10 règles d'or que tout le personnel puisse comprendre.	Directeur international de la GRS et Comité de gestion des risques	Déc-27	* Audit interne pour la vérification de la sensibilisation du personnel aux règles d'or - 80 % de prise de conscience minimale. -* Les règles d'or sont clairement affichées sur le site web, dans les bureaux internes, les bureaux nationaux du personnel.
3.3	Comité de gestion des risques en place et actif.	Directeur des opérations	Fév.-26	* Membres du groupe confirmés dans toutes les fonctions. * Historique des réunions trimestrielles, procès-verbaux et minutes, partagés avec l'équipe de direction exécutive.

Orientation stratégique 4 : Signalement, réflexion et révision

Résultat : Toutes les parties prenantes ont pris conscience du besoin de signaler les préoccupations, les incidents, et les incidents évités de justesse, et comptent sur les cadres supérieurs pour les contrôler et les traiter régulièrement.

N°	Objectif	Qui est responsable	Date d'échéance	Mesures pour réussir
4.1	Développer des mécanismes de commentaires pour le signalement des incidents, des incidents évités de justesse et les préoccupations.	Directeur international de la GRS et Comité de gestion des risques	Déc-27	* Les mécanismes de commentaires développés sont utilisés régulièrement par tout le personnel. * Journal régulièrement mis à jour de tous les incidents, les incidents évités de justesse et les préoccupations.
4.2	Révision et réflexion sur les incidents, les incidents évités de justesse et les préoccupations.	Directeur international de la GRS et Comité de gestion des risques	Déc-27	* Journal des actions désignant clairement les responsables d'actions, et rapports sur les étapes de progression en place. * Révision semestrielle sur les accidents graves et analyse des tendances complétées et partagées avec les responsables exécutifs.

Orientation stratégique 5 : Meilleures pratiques

Résultat : L'organisation est à jour, elle suit les bonnes pratiques, elle partage et collabore avec d'autres intervenants du secteur.

N°	Objectif	Qui est responsable	Date d'échéance	Mesures pour réussir

5.1	Interaction, communication et collaboration dans le secteur et avec les autres secteurs.	Directeur international de la GRS et Comité de gestion des risques/ Groupe de travail	Déc-26	* Participation à des forums et des groupes de GRS importants dans le secteur, tel que le GISF. * Relations établies avec les professionnels de GRS hors du secteur. Vérifications trimestrielles/ semestrielles consignées dans les minutes et partagées avec le comité de gestion des risques.
5.2	Comparaison et évaluation régulières des produits.	Directeur international de la GRS et Comité de gestion des risques	Déc-26	* Contrôle externe des pratiques de devoir de diligence mises en place conformément aux normes ISO en utilisant un fournisseur externe. Contrôle interne de l'analyse comparative du processus des bonnes pratiques défini et effectué tous les 18 mois. * Partage des résultats des audits/ contrôles, avec la direction exécutive et communiqués à l'ensemble du personnel avec les points d'action de suivi.

D'après le modèle fourni par Draper, R, (2014), Comment écrire un plan de sécurité stratégique https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

Outil 2
Comment rationaliser votre stratégie GRS

Vision	Définir votre vision. Décider d'un délai spécifique, pratique pour l'organisation, et se poser les questions suivantes : Quelle est l'évolution envisagée pour la GRS dans les cinq, dans votre organisation ? Quel public ciblez-vous ? Quelle vision voulez-vous donner de la GRS ? Comment allez-vous réaliser votre objectif ? **N'oubliez pas :** • Utiliser un langage simple qui peut être compris pas les personnes de tous horizons. • Votre vision doit être attirante et inspirer les gens pour qu'ils s'engagent. • Elle doit avoir un large contexte. • Elle doit être écrite au présent de l'indicatif.

Indicateurs/ Analyse des données	Il est important de pouvoir justifier votre énoncé de vision. Il peut inclure des chiffres et des indicateurs qui vont déterminer si, au final, la stratégie GRS a eu l'impact prévu (voir le Chapitre 6). **Les responsables de la stratégie GRS doivent se poser les questions suivantes :** • Quel est le nom de l'indicateur de mesure et quelle image de l'organisation va-t-il donner ? • Quel type de données doivent être produites à partir de l'indicateur et où trouver ces données ? • Quel type de tableau ou de visuel mettent le mieux en valeur les données ? • Quelles sont les différentes façons d'interpréter la mesure ?
Analyse SWOT	Le sigle SWOT signifie, points forts (*Strengths)*, points faibles (*Weaknesses*), opportunités (*Opportunities*), et menaces (*Threats*). L'analyse SWOT est un autre outil efficace de planification, les membres proposent, établissent la liste, et évaluent les points forts, les points faibles, les opportunités, et les menaces de leur organisations. L'analyse SWOT est un outil très efficace pour évaluer et analyser la santé de la GRS en place dans votre organisation. L'analyse SWOT peut être très utile pour vérifier l'approche de la GRS dans l'ensemble de la stratégie de votre organisation, et déterminer les points forts, les points faibles, les opportunités et les menaces pour aligner, le cas échéant, la stratégie GRS de l'organisation. (Voir L'outil 4, Modèle d'analyse SWOT).
Analyse PESTLE	Cette analyse est utilisée pour identifier les menaces et les points faibles en plus de l'analyse SWOT. La première étape d'une analyse PESTLE consiste à identifier tous les facteurs externes pouvant avoir un impact sur le travail de votre organisation. Au cours de l'analyse, les facteurs suivants sont évalués : Politique, économique, social, technologique, juridique, environnemental.
Diagramme d'affinité et de corrélation	Les résultats d'une analyse SWOT, nécessitent souvent la mise en place de projets stratégiques internes. Un diagramme d'affinité permet de rassembler et d'organiser un grand nombre d'éléments dans des catégories semblables afin de mieux les gérer. Faire un diagramme d'affinité requiert aux responsables des équipes de noter sur des post-it les initiatives ou les projets à venir identifiés par l'analyse SWOT. L'équipe doit ensuite trier ces notes par thèmes spécifiques avant d'assigner les projets à une ou plusieurs fonctions spécifiques. Cette pratique facilite et identifie les liens entre les fonctions et permet de désigner les responsables d'actions de manière logique.
Analyse du portefeuille	Identifier les différentes stratégies utilisées pour atteindre les objectifs de GRS par le passé. Les classer ensuite dans les catégories suivantes : « Star » (si la mise en place est réussie), « Fondation » (si la stratégie a servi de socle au déploiement des objectifs de GRS), « Point d'interrogation » (nouvelles stratégies non mises en place) et « Fiasco » (stratégies qui, après essai, ont échoué). Ces classements permettent de savoir sur quelles méthodes se concentrer ou quelles sont celles qu'il faut écarter ou revoir.

Outil 3
Modèle de planification de la GRS

OBJECTIFS DIRECTEURS	Pourquoi mettre en place une GRS ? Quel objectif voulons-nous atteindre ? Quels avantages pensons-nous en tirer ?
ÉLÉMENTS LES PLUS CRITIQUES DU PROCESSUS DE GRS POUR NOTRE ORGANISATION	Quels sont les éléments du cadre GRS les plus importants pour nos objectifs ?
APPROCHE POUR L'ADAPTATION DES PRINCIPES GRS À LA CULTURE ET AUX BESOINS DE L'ORGANISATION	Comment pouvons-nous intégrer la GRS aux processus déjà en place le plus efficacement possible ? Allons-nous former un nouveau comité sur les risques ou utiliser un forum existant pour discuter des risques ? Comment allons-nous former les responsables des risques ? Comment allons-nous inclure la GRS dans la planification stratégique et du budget ? Comment allons-nous mobiliser notre conseil d'administration ?
PLAN POUR AUGMENTER PROGRESSIVEMENT LA VALEUR DE GRS POUR NOTRE ORGANISATION	Comment et quand allons-nous développer la GRS pour augmenter la valeur qu'elle apporte à notre organisation ?

Outil 4
Modèle d'analyse SWOT

POINTS FORTS	POINTS FAIBLES
Que faisons-nous de bien dans le cadre de l'approche et du contexte actuels de la GRS ? Quelles ressources internes ou capacités avons-nous ou dans quelles ressources pouvons-nous puiser ? Par exemple, une bonne culture autour de la GRS, du personnel de GRS expérimenté, des outils d'évaluation des risques, d'un programme fort d'apprentissage et de développement.	Quels domaines du cadre actuel de GRS nécessitent une amélioration ? De quelles ressources ou formations manquons-nous ? Par exemple, une formation inadéquate à la gestion de crise, un manque de compréhension et d'engagement dans la GRS, des technologies obsolètes, une pauvre infrastructure.
OPPORTUNITÉS	**MENACES**
Quelles sont les opportunités que la GRS pourraient saisir ou dont elle pourrait tirer avantage ? Y-a-t-il des sites dans lesquels la GRS pourrait atteindre tous les objectifs de l'organisation/ satisfaire aux objectifs stratégiques ? Par exemple, les technologies émergentes, de nouveaux partenariats ou opportunités de réseautage.	Qu'est-ce qui peut menacer notre efficacité durant la mise en œuvre de la GRS dans l'organisation ? Par exemple, le maintien en fonction du personnel, les violations de la cybersécurité, les domaines d'intervention dans des contextes à haut risque, l'épuisement du personnel.

Outil 5
Exemple de déclaration d'attitude face au risque

Exemple 1 :

Pour atteindre les objectifs stratégiques de [définir] ...., il est inévitable que les activités opérationnelles *[inclure des exemples]* .... exposent le personnel à certaines menaces. L'organisation s'efforce de réduire le niveau de risque lié à ces menaces en employant des moyens efficaces de gestion des risques de sécurité.

Les risques sont considérés comme excessifs lorsque la possibilité d'un incident critique est plus probable que possible, en tenant compte des mesures d'atténuation des risques mises en application.

Un incident critique peut causer les problèmes suivants :

- un membre du personnel ou du personnel indirect souffre de douleurs physiques ou psychologiques graves ; ou
- les finances de l'organisation ou sa réputation ont essuyé de graves dommages.

..... travaille dans les environnements les plus compliqués et isolés. Lorsque les besoins programmatiques sont importants, ... doit accepter un plus haut niveau de risque. Dans de telles situations, une plus grande priorité doit être donnée à la gestion des risques de sécurité.

.....d'attitude face au risque prend toujours en compte les objectifs du programme, l'importance des objectifs à atteindre et la capacité à gérer les menaces, ainsi que l'impact d'autres facteurs stratégiques (tel que les relations clés et les intérêts des donateurs). Les responsables des risques décident au cas par cas, si les objectifs du programme spécifique et les résultats attendus justifient d'accepter le niveau de risque évalué.

Exemple 2 :

..... reconnaît que l'organisation travaille dans des environnements où le risque ne peut pas être totalement éliminé. Néanmoins, toutes les mesures pratiques doivent être prises pour réduire autant que possible les niveaux de risque.

Le niveau de risque résiduel, qui reste après que de telles mesures ont été mises en place, est acceptable seulement s'il est justifié par l'impact humanitaire sur les opérations.

Lorsque les risques non utiles ont été éliminés, et que l'activité peut être poursuivie car elle est jugée intéressante, les membres du personnel doivent être préparés à accepter le niveau de risque résiduel.

Exemples fournis par International Location Safety

Outil 6
Définir une approche organisationnelle des risques

Tolérance au risque

La tolérance du risque est un niveau acceptable de variation de l'attitude/ l'appétence au risque de l'organisation, en fonction de circonstances spécifiques (voir la section 1.5). Elle est apparentée au seuil de risque de l'organisation (c'est-à-dire, la quantité de risque qu'une organisation peut prendre avant que sa capacité à remplir sa mission ne soit trop largement impactée).

Définir votre approche des risques :

- Établir des paramètres clairs afin que les équipes puissent travailler dans le cadre de ces paramètres.
- Permettre le traitement systématique des risques.
- Se prémunir contre l'effondrement de l'organisation.

Processus :

1. **Définir le contexte :** Fournir une brève explication sur la façon dont les risques de GRS sont liés à- ou peuvent avoir un impact sur- l'ensemble de la stratégie de l'organisation en fonction de sa mission, ses buts, ses objectifs, et son contexte opérationnel. Faut-il prendre en considération des facteurs externes ?
2. **Identifier les limites :** Spécifier, clairement pourquoi il existe une attitude de tolérance zéro, pourquoi il faut adopter une attitude prudente, et pourquoi, dans certaines circonstances, un niveau plus élevé d'acceptation du risque peut être justifié (par exemple, selon les exigences des donateurs, des sites des programmes à haut risque).
3. **Définir des indicateurs :** Définir les indicateurs de risque clés utilisés pour évaluer si l'organisation exerce ses activités opérationnelles dans le cadre de- ou hors des seuils de risque. Ces indicateurs aident aussi à déterminer un plan d'actions concernant la gestion des différents risques.

Pour vérifier que l'attitude face au risque est proportionnée, utiliser le registre des risques organisationnels afin de savoir quelles sont les principales menaces. Il est possible de pratiquer ainsi pour chaque fonction de l'organisation. Évaluer l'impact et la probabilité que de telles menaces se produisent. Vous pouvez utiliser les définitions établies ou créer les vôtres. Voici un exemple ci-contre.

Probabilité

Score	Terme	Définition
1	Très faible	Il est très peu probable que la menace se concrétise.
2	Faible	Il est improbable que la menace se concrétise
3	Moyen	La menace est possible.
4	Élevé	Il est probable que la menace se concrétise.
5	Très élevé	Probabilité très élevée que la menace se concrétise.

Impact

Score	Terme	Définition
1	**Très faible**	Blessures insignifiantes ou peu d'effets sur la santé, pertes financières insignifiantes (<1 000 £), interruption de l'activité insignifiante (pas de perte de jours de travail), aucun danger réputationnel, tous des impacts réversibles.
2	**Faible**	Blessures minimes ou effets minimes sur la santé, pertes financières minimes (<5 000 £), interruption de l'activité minime (<1 jour de perte de travail), danger réputationnel minime, impacts pratiquement tous réversibles.
3	**Moyen**	Blessures modérées ou effets modérés sur la santé, pertes financières modérées (<10 000 £), interruption de l'activité modérée (de 1 à 2 jours de perte de travail), danger réputationnel modéré, impacts partiellement réversibles.
4	**Élevé**	Invalidité permanente ou multiples hospitalisations, effets majeurs sur la santé, pertes financières majeures (de 10 000 £ à 50 000 £), interruption de l'activité majeure (de 3 à 6 jours de perte de travail), exposition majeure de la réputation avec impact négatif, quelques impacts réversibles.
5	**Très élevé**	Décès, multiples incapacités ou hospitalisations permanentes, pertes financières importantes (>50 000 £), interruption importante de l'activité (>6 jours de perte de travail), exposition majeure de la réputation avec impact négatif, assistance extérieure nécessaire pour contenir le risque, impacts importants.

Les reporter sur une matrice de risque et surveiller continuellement :

Probabilité de menace	Impact de la menace				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	1	2	3	4	5
Faible	2	4	6	8	10
Moyen	3	6	9	12	15
Élevé	4	8	12	16	20
Très élevé	5	10	15	20	25

Les zones vertes sont incluses dans l'attitude face au risque de l'organisation. Elles peuvent être gérées selon des mécanismes normaux.

Les zones ambre sont à la limite de l'attitude face au risque de l'organisation, mais dans la limite de la tolérance du risque. Ces dernières doivent être signalées afin d'être traitées, et il pourrait être nécessaire de revoir les plans d'urgence.

Les zones rouge sont hors des seuils de risque de l'organisation. Elles doivent être signalées pour action immédiate afin d'améliorer les contrôles.

Source : International Location Safety

Outil 7
Exemple Termes de référence pour le Comité de gestion des risques

Sujets de réunion

Le Comité de gestion des risques travaille pour s'assurer qu'une ONG identifie proactivement et gère les risques qui pèsent sur son personnel. Il s'assure que l'ONG travaille en permanence pour le maintien et l'amélioration de la sécurité, le cas échéant, en éliminant les problèmes et les risques.

Les responsabilités et les tâches du groupe sont :

- Responsable du cadre de gestion de la sûreté et de la sécurité et des stratégies.
- Approuver toutes les demandes de déplacement d'un niveau de menace élevé ou très élevé.
- Effectuer les vérifications après un incident ou en situation de crise.
- Gérer la conformité du cadre de gestion des risques de sécurité.
- Approuver les activités et les priorités en gestion des risques.
- Assurer la gestion des risques de sécurité appropriée, et le financement de la crise.
- Approuver les communications et les messages de sécurité destinés au personnel.

Le groupe fournit à toutes les fonctions la possibilité que leurs équipes signalent elles-mêmes les problèmes. Il garantit que les solutions pour l'identification des risques englobent les besoins de l'organisation.

Personnes présentes

Rôle	Rôle du comité
	Président/ Membre du comité
	Vice-président/ Membre du comité
	Membre du comité
	Membre du comité
	Membre du comité

Planning

a. La réunion du Comité de gestion des risques a lieu tous les mois.

b. La présidence ou tout membre du comité peut organiser une réunion d'urgence si les circonstances l'exigent.

c. Le lieu de réunion est confirmé par la présidence à chaque nouvelle réunion.

d. La durée de la réunion est de 90 minutes.

Programme de la réunion

Sujet	Référence du document	Présenté par	Actions
Programme de la réunion		Président	
Incidents depuis la dernière réunion du Comité de gestion des risques	Rapports d'incidents/ rapport sur les leçons apprises	Président/ Membre du comité	Mise à jour de la base de données mondiale et/ ou du registre des risques si nécessaire
Mise à jour sur les actions du dernier SRMG	Minutes de la réunion	Président/ Membre du comité	
Principales réalisations, problèmes ou risques liés à la gestion des risques de sécurité		Président/ Membre du comité	
Révisions des formulaires de déplacement à très haut risque (si nécessaire)		Membre du comité	
Prochaine réunion		Président	
Toute autre activité		Président	

Termes

a. Le Président rapporte au Directeur général/ Conseil d'administration si nécessaire.

b. Chaque membre du comité dispose d'un droit de vote.

c. Au moins trois membres du comité doivent être présents pour atteindre le quorum.

d. Assister en présentiel n'est pas obligatoire, mais préférable. Assister par vidéoconférence ou audioconférence est accepté.

e. Si des membres du comité sont absents, ils sont autorisés à être remplacés.

f. Les personnes présentes sont autorisées à faire des recommandations dans le contexte et les limites de leurs domaines de connaissance.

g. En l'absence du Président et du Vice-président, la réunion doit être reportée à une autre date.

h. Les décisions sont prises à l'unanimité des membres du comité et sont enregistrées.

i. Les parties invitées peuvent proposer une décision au Comité, si une telle décision est adoptée à une réunion précédente.

Responsabilités et autorités

a. Organiser un forum confidentiel pour identifier les problèmes/ risques pesant sur l'organisation ou les actions des départements qui peuvent affecter la sécurité de l'organisation.

b. S'assurer que le travail du groupe de travail améliore continuellement la sûreté et la sécurité.

c. Assumer les responsabilités portant sur le cadre et les stratégies de gestion des risques de sécurité de l'organisation, et la signature des protocoles et des outils.

d. Approuver toutes les demandes de déplacement d'un niveau de menace élevé ou très élevé.

e. Effectuer les vérifications après un incident ou en situation de crise.

f. Gérer la conformité du cadre de gestion des risques de sécurité.

g. Approuver les activités et les priorités en gestion des risques.

h. Assurer la gestion des risques de sécurité appropriée, et le financement de la crise.

i. Approuver les communications et les messages de sécurité destinés au personnel.

j. Lorsque le risque légal et numérique peuvent aggraver la menace qui pèse sur le personnel ou les personnes sous les instructions de l'organisation, le prendre en compte dans les stratégies de gestion des risques et les mesures de réduction des risques.

k. Vérifier et accepter les changements des termes de référence pour le cadre de gestion des risques de sécurité.

Exemple fourni par International Location Safety

Outil 8
Modèle de plan de développement et d'apprentissage

D'après le modèle des compétences du 3e secteur du Conseil national des organismes bénévoles d'Angleterre (NCVO) : Analyse des besoins en formation

Objectif organisationnel	Connaissances et compétences requises	Qui participe ?	Activités/ méthodes d'apprentissage et de développement	Quelles sont les modalités d'évaluation ?	Coût	Date

Outil 9
Exemple de matrice pour la formation stratégique

Cet outil peut être adapté ou étendu au niveau opérationnel pour refléter les besoins/ date de fin/ niveau de compétence dans chaque domaine.

Description	Nom du fournisseur (interne/ externe)	Responsables stratégiques	Directeurs régionaux	Directeurs pays	Points focaux pour la sécurité	Tout le personnel
Cadre de sécurité						
Créer des procédures (par exemple, des plans de sûreté et de sécurité au niveau du pays, des risques relatifs au pays, des registres, des plans de gestion des incidents)						
Évaluation des risques						
Formation du personnel à la sécurité sur le terrain/ sensibilisation à la sécurité sur le terrain						
Formation à la sûreté et à la sécurité durant les voyages						
Atelier de gestion de crise						
Premiers secours						
Gestion de la résilience et du stress						
Formation à la gestion des risques de sécurité						
L'importance du devoir de diligence						
Signalement des incidents de sécurité						
Cybersécurité						
Formation à l'intégrité et à l'anticorruption						
Formation à l'antisubornation et à l'anticorruption						
Surveillance						

- Prioritaire
- Dans les 12 mois
- Non requis

Exemple fourni par International Location Safety

Outil 10
Modèle de théorie du changement

Contexte : Quel est le contexte ou la raison de ce changement ?

Objectifs : Comment reconnaître le succès ?

Contributions et activités	Production	Mécanisme de changement	Résultats	Impacts
Contributions Quels seront les coûts, le personnel et les autres ressources nécessaires ?	Quels résultats, produits, leçons, inspections ou améliorations tangibles sont produites ?	Quelles actions sont nécessaires pour parvenir aux changements ? Est-ce que vous éliminez les désaccords, changez les comportements, etc. ?	**Court terme** Quels seront les avantages et les résultats plus généraux, indicateurs avancés et indicateurs retardés ?	Quels sont les impacts et comment s'inscrivent-ils dans les priorités régionales et gouvernementales ?
Activités Quelles activités, formations ou orientations ?			**Long terme** Quels seront les changements durables et permanents, et quels paramètres de mesure seront utilisés pour les mesurer ?	

Évaluation des preuves : Quel est le point fort de la base factuelle existante pour ce changement ?

Hypothèses : Qu'est-ce qui est supposé faire partie du plan ?

Éventuelles conséquences imprévues ? Y-aurait-t-il d'autres résultats qui pourraient résulter de ce projet ?

Adapté d'un exemple fourni par le UK Foreign, Commonwealth and Development Office (FCDO)

Outil 11
Modèle de cadre logique

	RÉSUMÉ DU PROJET	INDICATEUR Comment est-il calculé ?	SOURCE DES DONNÉES Comment est-elle évaluée ?	RISQUES/ HYPOTHÈSES
Objectif				
Résultats				
Produc-tion				
Activité				

Source : Tools4Dev

Outil 12
Modèle de planification MEAL

Indicateur	Activité MEAL spécifique	Qui est impliqué(e)	Qui est responsable	Principales étapes	Durée prévue	Coût
Culture de l'organisation en ce qui concerne l'engagement avec compréhension de la GRS	Enquête de perception adressée à tout le personnel	Communications à l'informatique, aux ressources humaines et à la GRS	GRS et communications	**T1 :** Remet en question la conception proposée, le système développé en ligne **T2 :** Enquête en cours d'achèvement **T3 :** Résultats de l'enquête analysés et présentés	**T1-T3**	**Temps accordé au personnel :** Cinq jours pour le développement de l'enquête et le système informatique, et pour effectuer le contrôle qualité 30 minutes accordées à chaque membre du personnel pour répondre à l'enquête Trois jours pour analyser et présenter les conclusions **Coût financier :** Adhésion au système d'enquête électronique 250 £
Engagement par rapport aux comptes-rendus sur les mécanismes de GRS	Incident/ incident évité de justesse/ journal des préoccupations (accès par l'application mobile) avec des liens vers les actions et les responsables concernés	Programmes RH, GRS, TI, Financier, Légal	GRS et TI	**T1 :** Mise en place et déploiement du système de journalisation **T2 :** Formation au renforcement des capacités pour tout le personnel **T3 :** Système en direct **T4 :** Résultats et premières actions et analyses	**T1-T2 : Développement et mise en place** Permanent : Examen trimestriel et réflexions	**Temps accordé au personnel :** 30 jours pour le développement et la mise en place Une heure de formation pour tout le personnel **Coût financier :** 3 000-5 000 £ pour le système basé sur l'application 1 000 £ pour la formation extérieure
Engagement et communications sur les problèmes/ préoccupations concernant la GRS	Mise en place d'une journalisation en ligne de toutes les réunions, ordres du jour et minutes concernant la GRS	TI, GRS	GRS	**T1 :** Mise en place de systèmes internes **T2 :** Formation en renforcement des capacités, ordres du jour confirmés **T3 :** Compilation, réflexion et révision continues	**T1-T2 : Développement et mise en place** Permanent : Examen trimestriel et réflexions	**Temps accordé au personnel :** Deux jours pour la mise en place Une heure de formation en renforcement des capacités pour le personnel clé de GRS **Coût financier :** 0 £
Vérification physique des ressources, de l'équipement et des mesures GRS en place	Conception et déploiement de la structure d'audit interne	Programmes GRS, TI, Légal	GRS et programmes	**T1 :** Mise en place d'un système et d'un processus d'audit interne **T2 :** Formation en renforcement des capacités pour tous les responsables d'audit et déploiement de tout le personnel **T3 :** Compilation, réflexion et révision continues	**T1-T2 : Développement et mise en place** Permanent : Examen trimestriel et réflexions	**Temps accordé au personnel :** 15 jours de mise en place Trois heures de formation pour chaque responsable d'audit, une heure de formation pour tout le personnel **Coût financier :** Modifications et développement du système TI - 1 000 £

Indicateur	Activité MEAL spécifique	Qui est impliqué(e)	Qui est responsable	Principales étapes	Durée prévue	Coût
Engagement et communications sur les problèmes/ préoccupations concernant la GRS	Modifier les modèles de rapport de programme pour inclure la section de commentaires sur la GRS liée au journal des incidents, des incidents évités de justesse, et des préoccupations.	Programmes GRS, TI	Programmes et GRS	**T1 :** Modifications apportées **T2 :** Renforcement des compétences avec les responsables des programmes **T3 :** Déploiement **T4 :** Compilation, réflexion et révision continues	**T1-T2 : Développement et mise en place** Permanent : Examen trimestriel et réflexions	**Temps accordé au personnel :** 10 jours pour le développement et la vérification Trois heures de formation pour chaque responsable de programme **Coût financier :** 0 £
Renforcement des compétences eu égard à la GRS	Matrice de formation et journal développé, renseigné et intégré	RH, GRS, TI, Finance	RH et GRS	**T1 :** Analyse des besoins en formation effectuée. Développement de la matrice et configuration du journal **T2 :** Début du programme de formation **T3 :** Système en direct **T4 :** Résultats et premières actions et analyses	**T1-T2 : Développement et mise en place** Permanent : Examen trimestriel et réflexions	**Temps accordé au personnel :** Huit jours pour le développement et la mise en place Besoin en formation continue dépendant de l'analyse des besoins en formation **Coût financier :** Dépend des fournisseurs de formations

Exemple fourni par International Location Safety

Bibliographie

Général

Breckenridge, M.-J., Czwarno, M., Duque-Díez, M., Fairbanks, A., Harvey, P., and Stoddard, A. (2023). Aid worker security report 2023. Security training in the humanitarian sector: Issues of equity and effectiveness. Humanitarian Outcomes. https://www.humanitarianoutcomes.org/AWSR_2023

Hermann, E., & Oberholzer, S. (2020). 'Security Risk Management and Risk Aversion in the Humanitarian Sector. Assessing Decision-Making Processes in Local and International Humanitarian NGOs'. Geneva: ICVA. https://www.icvanetwork.org/uploads/2021/07/Security_Risk_Management_May2020-1.pdf

Humanitarian Practice Network (HPN). (2010). Good Practice Review: Operational Security Management in Violent Environments. Number 8 (new edition). Overseas Development Institute. https://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Chapitre 1

Chapple, M, (2023): 'Risk appetite vs risk tolerance; How are they different', Tech Target. https://www.techtarget.com/searchcio/feature/Risk-appetite-vs-risk-tolerance-How-are-they-different

Datminr, (2022), 'Understand and plan for the corporate risk landscape'. https://www.dataminr.com/resources/ebook/understand-and-plan-for-the-corporate-risk-landscape

Donovan, L (2022), 'What is risk appetite and how do you implement it?', Risk Leadership Network. https://www.riskleadershipnetwork.com/insights/what-is-risk-appetite-and-how-do-you-implement-it

Draper, R (2014), 'How to write a strategic security risk management plan', LinkedIn https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

Khushi, S, (2017), 'Strategic planning for NGOs: A guide to understanding the basics of strategic planning', LinkedIn. https://www.linkedin.com/pulse/strategic-planning-ngos-guide-understand-basics-samina-khushi/

Simpson, K. & Randall, I (2020). 'Systemcraft: A primer', Wasafiri. https://u05.88f.myftpupload.com/wp-content/uploads/2020/10/Wasafiri-SystemCraft-2020-Small.pdf

UN Programme Criticality Steering Group (2016), United Nations System Programme Criticality Framework, CEB/2016/HLCM/23. https://programmecriticality.org/Static/index.html

USAID (2022). 'USAID Risk Appetite Statement: A Mandatory Reference for ADS Chapter 596'. https://www.usaid.gov/sites/default/files/2022-12/596mad.pdf

Chapitre 2

Mind Tools Article, 'The RACI Matrix: Structuring accountabilities for maximum efficiency and results'. https://www.mindtools.com/agn584l/the-raci-matrix

Von Moltke, N, (2024), 'RACI Template and Ultimate 2024 Guide to the RACI Matrix', Academy to Innovate. https://www.aihr.com/blog/raci-template/

Chapitre 3

IEC 31010:2019: Risk Management: Risk Assessment Techniques. https://www.iso.org/standard/72140.html

Swiss Centre of Competence for International Cooperation (CINFO) and GISF, Duty of Care Self-Assessment Tool. https://dutyofcare.cinfo.ch/index.html

3.2 Programmes/ Opérations

Frontline Defenders, Workbook on Security. https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

GISF Security Toolbox, 2. Acceptance Analysis. https://www.gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/

GISF. (2021) Achieving Safe Operations through Acceptance: challenges and opportunities for security risk management. Global Interagency Security Forum (GISF). https://www.gisf.ngo/wp-content/uploads/2021/12/Achieving_Safe_Operations_through_Acceptance_challenges_and_opportunities_for_security_risk_management.pdf

Larissa Fast, L., Finucane C., Freeman F., O'Neill M., Rowley E., (2011) The Acceptance Toolkit, Save the Children. https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf

Morrow, E. (2023) Humanitarian Access & Security Management: considerations for staff security, GISF blog. https://www.gisf.ngo/blogs/humanitarian-access-security-management-considerations-for-security-staff/

Stoddard, A., Czwarno, M., and Hamsik, L. (2019). NGOs & risk: Managing uncertainty in local-international partnerships (global report). Humanitarian Outcomes. https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships

3.3 Finance

Global Interagency Security Forum (GISF). (2013). The cost of security risk management for NGOs. https://www.gisf.ngo/resource/the-cost-of-srm-for-ngos/

Sweeney, A, (2019), 'Securing aid worker safety through effective budgeting', Crisis Response, October 2019 | Vol: 14 | issue 4 https://www.gisf.ngo/wp-content/uploads/2019/11/Securing-Aid-Worker-Safety-Through-Effective-Budgeting.pdf

3.4 Communications

Foulkes, I, (2022), Misinformation campaign against the International Committee of the Red Cross in Ukraine, BBC News. https://www.bbc.com/news/world-europe-60921567

GISF and Cornerstone OnDemand Foundation, (2019), Security Risk Management Toolkit: Strategies. https://gisf.ngo/wp-content/uploads/2020/03/Planning-security-risk-management-strategies-and-systems.pdf

Internews, (2019), Managing Misinformation in a Humanitarian Context. https://internews.org/wp-content/uploads/2021/02/Rumor_Tracking_Mods_3_How-to-Guide.pdf

Leyland, J., Tiller, S., and Bhattacharya, B. (2023). Misinformation in humanitarian programmes: Lessons from the MSF Listen experience. Journal of Humanitarian Affairs, 5(2).

Oh, S., Adkins, T. (2018), Disinformation Toolkit, InterAction. https://www.interaction.org/wp-content/uploads/2019/02/InterAction_DisinformationToolkit.pdf

3.5 TI

Dugan, S. (2022), 'Cyberattacks; a real threat to NGOs and not-for-profits', Reliefweb. https://reliefweb.int/report/world/cyberattacks-real-threat-ngos-and-nonprofits

GISF, (2020), Security to Go: Module 4 Digital Security. https://gisf.ngo/wp-content/uploads/2020/11/GISF_Security-to-Go_Module-4_Oct20.pdf

ICRC, (2024), Cyberattack on ICRC: What we know. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Kumar M. (2017), Digital Security of LGBTQ+ Aid Workers: Awareness and Response. https://www.gisf.ngo/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/

Stine K., Quinn S., Witte G., Gardner R.K., (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM), National Institute of Standards. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

3.6 HR

Arthur, T and Moutard, L, (2022). Toward inclusive security risk management: the impact of 'race', ethnicity and nationality on aid workers' security. Global Interagency Security Forum (GISF). https://gisf.ngo/wp-content/uploads/2022/05/Towards-Inclusive-Security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security.pdf

GISF Inclusive Security Podcast Series E1: Introducing a person-centred approach. https://gisf.ngo/resource/inclusive-security-e1-introducing-a-person-centered-approach/

GISF, (2018), Managing the Security of Aid Workers with Diverse Profiles. https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/

GISF (2017), Security-to-Go Toolbox: Module 12 People Management, C Williamson. https://gisf.ngo/resource/people-management-security-to-go-module/

Goldhill, O (2019), Palestine's head of mental health services says PTSD is a western concept, Quartz Journals. https://qz.com/1521806/palestines-head-of-mental-health-services-says-ptsd-is-a-western-concept

Goozee, H (2020), Decolonizing Trauma with Franzt Fanon, Oxford University Press. https://academic.oup.com/ips/article-abstract/15/1/102/5868933?redirectedFrom=fulltext

McKinsey & Company. (2023). What Is Psychological Safety? McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-psychological-safety

Persaud, C. (2014a). Gender and security: Guidelines for mainstreaming gender in security risk management. GISF. https://www.gisf.ngo/resource/ gender-and-security/

3.7 Légal

GISF, (2012), International agencies working with local partners, GISF Briefing Paper. https://gisf.ngo/resource/international-agencies-working-with-local-partners/

ISOS Global Duty of Care Benchmarking Report, 2015. https://www.internationalsos.co.id/duty-of-care

Merkelbach, M. and Kemp, E. (2011). Can you get sued? Legal liability of international humanitarian aid organisations towards their staff. Security Management Initiative. https://www.gisf.ngo/resource/ can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

Merkelbach, M. and Kemp, E. (2016). Duty of care: A review of the Dennis v Norwegian Refugee Council ruling and its implications. GISF. https://gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/

3.8 Sauvegarde

GISF Webinar | Intersection of Security and Safeguarding | Recording. https://gisf.ngo/resource/gisf-webinar-intersection-of-security-and-safeguarding-recording/

Mullin K., (2021), Launching the community-based safeguarding visual toolkit. https://www.interaction.org/blog/launching-the-safeguarding-community-visual-toolkit/

Safeguarding Resource and Support Hub (RSH). https:/ safeguardingsupporthub.org/

How-to note on implementing the safeguarding cycle. https://www.gisf.ngo/resource/how-to-note-on-implementing-the-safeguarding-cycle/

Essentials. https://safeguardingsupporthub.org/essentials

PSEA Glossary. https://safeguardingsupporthub.org/psea-glossary-clear-global

Introduction to safeguarding – RSH South Sudan. https://safeguardingsupporthub.org/sites/default/files/essentials/Essentials_What%20is%20safeguarding/Essentials_Introduction%20to%20safeguarding%20South%20Sudan.pdf

3.9 Voyages

ISO 31030: Travel Risk Management. https://www.iso.org/standard/54204.html

Chapitre 4

GISF (2022), NGO Security Collaboration Guide, Global Interagency Security Forum (GISF). https://www.gisf.ngo/long-read/ngo-security-collaboration-guide/

GISF. (2021) Partenariats et gestion du risque sécurité : guide d'action conjointe pour les organisations humanitaires locales et internationales. Global Interagency Security Forum (GISF). https://gisf.ngo/resource/partenariats-et-gestion-du-risque-securite-guide-daction-conjointe-pour-les-organisations-humanitaires-locales-et-internationales/

GISF. (2020) Partnerships and Security Risk Management: from the local partner's perspective. Global Interagency Security Forum (GISF). https://www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/

ISO 31000:2018 Risk Management. https://www.iso.org/standard/65694.html

UN Department for Safety and Security (UNDSS). (2015). Saving lives together. A framework for improving security arrangements among international non-governmental organisations/international organisations and the United Nations. https://www.gisf.ngo/wp-content/uploads/2020/02/2225-UNDSS-2015-Saving-Lives-Together-Framework.pdf

Williams C., (2020), Collaborative Security Risk Management: A case for local development, GISF Article. https://www.gisf.ngo/collaborative-security-risk-management-a-case-for-local-development/

Chapitre 5

Buth P., (2010), Crisis Management of Critical Incidents, GISF. https://www.gisf.ngo/resource/crisis-management-of-critical-incidents/

GISF and OSAC. (2023) NGO Crisis Management Exercise Manual: a guide to developing and facilitating effective exercises. Global Interagency Security Forum (GISF) and Overseas Security Advisory Council (OSAC). https://www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/

Kunal K., Eder P., LinkedIn Community, (2023), How do you foster a culture of risk awareness and accountability across different functions and levels? https://www.linkedin.com/advice/0/how-do-you-foster-culture-risk-awareness

Lucidchart, (2023), Top strategies for managing cross-functional teams. https://www.lucidchart.com/blog/managing-cross-functional-teams

Miller, R., (2018), Cross-functional teams impacting information security efforts, LinkedIn. https://www.linkedin.com/pulse/cross-functional-teams-impacting-information-security-richard-miller/?trk=public_profile_article_view

Nagele-Piazza L., (2018), Create a cross-functional team to combat data security issues, Society for Human Resource Management (SHRM) https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/cross-functional-team-to-combat-data-security-issues.aspx

White J., Gouveia B, Singer J, Josias M., Emerging trends and early lessons on crisis management and business resilience, S-RM Intelligence and Risk Consulting. http://www.s-rminform.com/srm-insights/crisis-management-business-resilience

Chapitre 6

Benjamin M., (2023), The benefits of real-time monitoring and evaluation, LinkedIn. https://www.linkedin.com/pulse/benefits-real-time-monitoring-evaluation-migolo-benjamin/

Data for Development, (2021), Ways you can integrate technology in monitoring and evaluation. https://datafordev.com/ways-you-can-integrate-technology-in-monitoring-and-evaluation/

International Rescue Committee (2021), Result Chain, Logframe and Theory of Change Terminology. https://rescue.app.box.com/s/e8sj6rep7hghs8j2yern8crxauavs6o8/file/775591027183

Gadkari M., (2023), What is Monitoring, Evaluation and Learning (MEL)?, Resonance Global. https://www.resonanceglobal.com/blog/what-is-monitoring-evaluation-and-learning-mel

Pasanen T., Barnett I, (2019), Supporting adaptive management, Overseas Development Institute. https://cdn.odi.org/media/documents/odi-ml-adaptivemanagement-wp569-jan20.pdf

Scotland's International Development Alliance, (2023), Monitoring, Evaluation and Learning (MEL) Guide. https://intdevalliance.scot/wp-content/uploads/2023/08/MEL_Support_Package_4th_June.pdf

The World Bank, (2004), Monitoring and Evaluation; Some Tools, Methods and Approaches. https://cnxus.org/wp-content/uploads/2022/04/WB_ME20ENG.pdf

The Monitoring and Evaluation Toolkit: An introductory toolkit for beginners, Article: 'What is M&E'. https://thetoolkit.me/what-is-me/

Turnbull M., Turvill E., (2012) Participatory Capacity and Vulnerability Analysis: A practitioner's guide, Oxfam GB. https://policy-practice.oxfam.org/resources/participatory-capacity-and-vulnerability-analysis-a-practitioners-guide-232411/

Wilsdon, N. Institute of Voluntary Action Research, 'Taking a strategic learning approach to evaluation'. https://www.ivar.org.uk/blog/taking-a-strategic-learning-approach-to-evaluation/

Nigeria
Une bénévole de Médecins Sans Frontières, travaille dans une clinique dans laquelle des personnes ont été déplacées.

gisf

Global Interagency Security Forum

GISF Research and Programmes
Tél. : +44 (0)20 7274 5032
E: research@gisf.ngo

www.gisf.ngo